# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-345864
(43)Date of publication of application : 14.12.2001

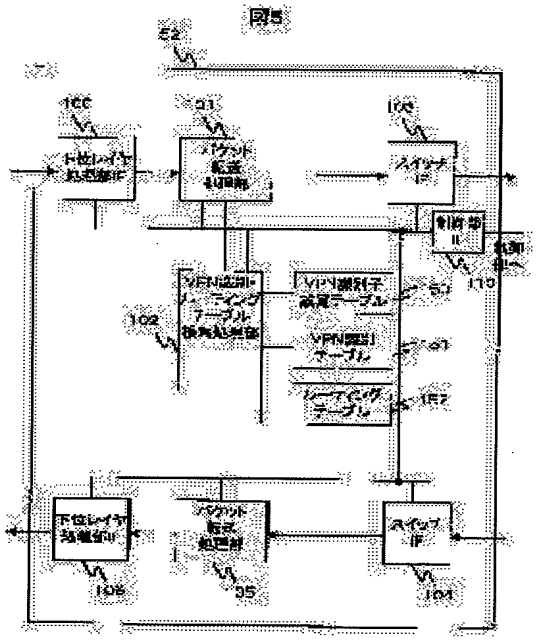
(51)Int.Cl. H04L 12/66
H04L 12/46
H04L 12/28
H04L 12/56

(21)Application number : 2000-170414
(22)Date of filing : 02.06.2000

(71)Applicant : HITACHI LTD
(72)Inventor : AKAHA SHINICHI
SAKAMOTO KENICHI
SUKAI KAZUO

## (54) ROUTER DEVICE, PACKET TRANSFER CONTROL METHOD, AND SETTING METHOD FOR VPN IDENTIFICATION INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a means for identifying to which virtual private network(VPN) a received packet belongs to in an edge router which accommodates the same line, when plural VPNs are multiplexed to this line.
SOLUTION: The VPN edge router is provided with a function for identifying the VPN, while using logical channel numbers multiplexed to the same line. Thus, the VPN can be identified by using the logical channel numbers multiplexed to a physical interface. Therefore, the number of VPN to be accommodated can be increased, without having to increase the number of physical lines.



LEGAL STATUS

[Date of request for examination] 16.02.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]
[Claim 1] The physical interface which holds the receiving circuit to which it is router equipment which can hold two or more virtual private networks (henceforth "VPN"), and multiplex [ of two or more logical channels ] was carried out, The logical channel identifier currently assigned to each logic-channel of two or more above-mentioned logical channels, The memory holding the table showing correspondence relation with the VPN name currently assigned to two or more above-mentioned VPN, When the packet transmitted through one logical channel in two or more above-mentioned logical channels is received, Router equipment characterized by having the processing section with which search the above-mentioned table and the above-mentioned receive packet judges it to be whether it belongs to which VPN among two or more above-mentioned VPN by using as a search key the logical channel identifier which the above-mentioned logical channel is assigned.
[Claim 2] Two or more physical interfaces with which it is router equipment according to claim 1, and a transmitting circuit is held, respectively, The address information of the packet used for each VPN correspondence of two or more above-mentioned VPN by each VPN, It has the memory holding the routing table showing correspondence relation with the information which identifies two or more above-mentioned physical interfaces. The above-mentioned processing section Router equipment characterized by determining whether to transmit the above-mentioned receive packet from which physical interface among two or more above-mentioned physical interfaces by searching the above-mentioned routing table by using as a search key destination address information stored in the header unit of the above-mentioned packet.
[Claim 3] It is router equipment which it is router equipment according to claim 2, the above-mentioned routing table holds the relation between the address information of the packet used by each VPN, and the header information given in case a packet is outputted, and the above-mentioned processing section uses as a search key destination address information stored in the header unit of the above-mentioned packet, and is characterized by to determine the packet header information which searches the above-mentioned routing table and is given to the above-mentioned receive packet.
[Claim 4] It is router equipment characterized by being router equipment given in any of claim 2 or claim 3 they are, and holding physically the above-mentioned table and the above-mentioned routing table on the same memory.
[Claim 5] It is router equipment which it is router equipment given in any of claim 1 thru/or claim 4 they are, and the above-mentioned receiving circuit is an Asynchronous Transfer Mode (ATM) circuit, and is characterized by the above-mentioned logical channel identifiers being VPI and VCI.
[Claim 6] It is router equipment which it is router equipment given in any of claim 1 thru/or claim 4 they are, and the above-mentioned receiving circuit is a Frame Relay circuit, and is characterized by the above-mentioned logical channel identifier being DLCI.
[Claim 7] It is router equipment which the packet encapsulated by the L2TP header as which it is router equipment given in any of claim 1 thru/or claim 4 they are, and the above-mentioned receiving circuit is specified by L2TP (Layer2 Tunneling Protocol) is transmitted, and is

characterized by the above-mentioned logical channel identifier being the information in a L2TP capsule header.
[Claim 8] It is VLAN as which it is router equipment given in any of claim 1 thru/or claim 4 they are, the above-mentioned receiving circuit is an Ethernet (trademark) circuit, and the above-mentioned logical channel identifier is specified by IEEE802.1Q. Router equipment characterized by being Tag.
[Claim 9] It is router equipment given in any of claim 1 thru/or claim 4 they are, and the above-mentioned receiving circuit is PPP. Over It is router equipment which the packet encapsulated by Ethernet (trademark) is transmitted and is characterized by the above-mentioned logical channel identifier being the information in the capsule header.
[Claim 10] It is router equipment which is router equipment given in any of claim 1 thru/or claim 9 they are, and is characterized by the ability to set up the correspondence relation between the above-mentioned logical channel identifier which the above-mentioned router equipment can be connected with a control terminal, and is held in the above-mentioned table from the above-mentioned control terminal, and the above-mentioned VPN name.
[Claim 11] It is router equipment. The 1st virtual private network (It is hereafter called "VPN".) The 1st local area network which belongs (it is called "LAN" below.) And the interface section which holds the circuit to which multiplex [ of the packet encapsulated with the same protocol ] is carried out, and it is transmitted from the 2nd LAN belonging to the 2nd VPN, Router equipment characterized by having a means to set up the identifier for identifying whether it belongs whether the packet which received from the 1st circuit of the above belongs to the 1st above VPN to the 2nd above VPN.
[Claim 12] It is router equipment which it is router equipment according to claim 11, and the above-mentioned protocol is an Asynchronous Transfer Mode protocol, and is characterized by the above-mentioned identifiers being VPI and VCI.
[Claim 13] A virtual private network which is router equipment and is different, respectively (It is hereafter called "VPN".) Two or more local area networks which belong (it is called "LAN" below.) from -- with the 1st interface section which holds the 1st circuit to which the packet encapsulated with the 1st protocol is transmitted The 2nd interface section which holds the 2nd circuit to which the packet encapsulated with the 2nd protocol from two or more LANs belonging to VPN which belongs to different VPN, respectively is transmitted, A means to set up the 1st identifier for identifying whether the packet which received from the 1st circuit of the above belongs to which VPN, The 1st identifier of the above is router equipment which has a means to set up the 2nd identifier for identifying whether the packet which received from the 2nd circuit of the above belongs to which VPN, and is characterized by the 2nd identifiers of the above differing.
[Claim 14] It is router equipment which it is router equipment according to claim 13, the 1st protocol of the above is an Asynchronous Transfer Mode protocol, the 1st identifier of the above is VPI and VCI, and the 2nd protocol of the above is a Frame Relay, and is characterized by the 2nd identifier of the above being DLCI.
[Claim 15] It is router equipment. The 1st virtual private network (It is hereafter called "VPN".) The 1st local area network which belongs (it is called "LAN" below.) from -- the packet encapsulated with the 1st protocol, and the packet encapsulated with the 1st protocol of the above from the 2nd LAN belonging to the 2nd VPN -- ** -- with the 1st interface section which holds the 1st circuit ******(ed) and transmitted The 2nd circuit to which the packet encapsulated with the 2nd protocol from the 3rd LAN belonging to the 3rd VPN is transmitted, The 2nd interface section which holds the 3rd circuit to which the packet encapsulated with the 2nd protocol of the above from the 4th LAN belonging to the 4th VPN is transmitted, A means to set up the 1st identifier for identifying whether it belongs whether the packet which received from the 1st circuit of the above belongs to the 1st above VPN to the 2nd above VPN, The 1st identifier of the above is router equipment which has a means to set up the 2nd identifier for identifying whether it belongs whether the packet which received from the 2nd circuit of the above and the 3rd circuit of the above belongs to the 3rd above VPN to the 4th above VPN, and is characterized by the 2nd identifiers of the above differing.

[Claim 16] It is router equipment characterized by being a physical interface number being router equipment according to claim 15, the 1st protocol of the above being an Asynchronous Transfer Mode protocol, for the 1st identifier of the above being VPI and VCI, for the 2nd protocol of the above being PPP over SONET, and for the 2nd identifier of the above identifying the 3rd circuit of the above, and the 4th circuit of the above.
[Claim 17] It is the packet transfer control approach in the router equipment which can hold two or more virtual private networks (henceforth "VPN"). The above-mentioned router equipment The logical channel identifier by which two or more logical channels hold the receiving circuit by which multiplex was carried out, and are assigned to each logic-channel of two or more above-mentioned logical channels, It has the table showing correspondence relation with the VPN name currently assigned to two or more above-mentioned VPN. The above-mentioned approach The packet transmitted through one logical channel in two or more above-mentioned logical channels is received. It is characterized by having the step which searches the above-mentioned table and judges whether the above-mentioned receive packet belongs to which VPN among two or more above-mentioned VPN by using as a search key the logical channel identifier which the above-mentioned logical channel is assigned.
[Claim 18] It is the packet transfer control approach which it is the packet transfer control approach according to claim 17, and the above-mentioned receiving circuit is an Asynchronous Transfer Mode (ATM) circuit, and is characterized by the above-mentioned logical channel identifiers being VPI and VCI.
[Claim 19] It is the setting approach of the VPN identification information in the router equipment which holds two or more local area networks (LAN) belonging to a virtual private network (henceforth "VPN") different, respectively. The above-mentioned router equipment receives the packet encapsulated with the 1st protocol from some LANs of two or more above-mentioned LANs, and the packet encapsulated with the 2nd protocol is received from other LANs of two or more above-mentioned LANs. Have memory and the packet which received the above-mentioned approach from LAN of a part of above sets the 1st identifier for identifying whether it belongs to which VPN as the above-mentioned memory. The 2nd identifier for identifying whether the packet which received from LAN besides the above belongs to which VPN is set as the above-mentioned memory, and it is characterized by the 2nd identifier of the above differing from the 1st identifier of the above.
[Claim 20] The setting approach of the VPN identification information characterized by having further the step which is the setting approach of VPN identification information according to claim 19, sets up the 1st table showing the correspondence relation between the 1st identifier of the above, and the VPN number currently assigned to VPN, and sets up the 2nd table showing the correspondence relation between the 2nd identifier of the above, and the VPN number currently assigned to VPN.
[Claim 21] It is the setting approach of the VPN identification information which it is the setting approach of VPN identification information given in any of claim 19 or claim 20 they are, the 1st protocol of the above is an Asynchronous Transfer Mode protocol, the 1st identifier of the above is VPI and VCI, and the 2nd protocol of the above is a Frame Relay, and is characterized by the 2nd identifier of the above being DLCI.
[Claim 22] The packet transfer control approach characterized by to have the step which is the packet transfer control approach in the router equipment which holds two or more virtual private networks (henceforth "VPN"), receives the IP packet to which the capsule header by the protocol equivalent to a layer 2 was given, and determines whether the IP packet which carried out [ above-mentioned ] reception belongs to which VPN using the information in the above-mentioned capsule header.
[Claim 23] Router equipment characterized by having a means to determine whether the IP packet which carried out [ above-mentioned ] reception belongs to which VPN using the information in the above-mentioned capsule header as the interface section which is router equipment which holds two or more virtual private networks (henceforth "VPN"), and receives the IP packet to which the capsule header by the protocol equivalent to a layer 2 was given.

[Translation done.]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the router equipment which is applied to router equipment, its packet transfer control approach, and the routing information setting approach in router equipment, especially builds the virtual private network (VPN:Virtual Private Network) in the Internet, its transfer control approach, and its setting approach.
[0002]
[Description of the Prior Art] When two or more networks in a company which exist in a different area conventionally were connected by the network, the company was building the network (that is, security was secured) isolated from the external network by interconnecting the network in a company by the dedicated line. However, when the dedicated line was used, there was a problem that network cost will go up. For this reason, it is cheap and the demand to the technique of building the imagination dedicated line network (it being hereafter called VPN:Virtual Private Network) of low cost using the Internet has increased with the spread of the Internet which can be used. This technique builds a dedicated network on the Internet virtually using the function of the lower layer of IP which IP (Internet Protocol) network offers, or IP. With this technique, also on IP network, it is safe and the network which was isolated from the external network and which can perform a certain QA can be built.
[0003] As a method which realizes VPN, it encapsulates at the entry of the network of the Internet Service Provider (hereafter referred to as ISP) which offers VPN, and there is a method which transmits based on this encapsulated header and transmits with the method which removes a capsule header at a network outlet on the network of ISP. By using the capsulation header of a VPN proper, VPN to which security was secured can consist of the interior of the Internet. As a concrete protocol of this capsulation, there are methods, such as IP capsulation, and MPOA (Multi Protocol OverATM), MPLS (Multi Protocol Label Switching), and the standardization is advanced in standardization organizations, such as a May, 2000 current and IETF.
[0004]
[Problem(s) to be Solved by the Invention] There are a global IP address and a private IP address in an IP address. A company can define a private IP address freely to a global IP address being what is globally set to a meaning. With the network in a company, a private IP address is used in many cases. Therefore, when a company uses a VPN service, it is desirable that a private IP address can be used. In this case, the same IP address may be used among two or more VPN. When the IP address between two or more VPN carries out batting, in order to process the packet of each VPN correctly, it is necessary, as for the router (for it to be hereafter called a VPN edge router) which holds LAN (Local Area Network) which is located in the entry of an ISP network and belongs to VPN, to hold the routing table for every VPN. A VPN edge router will judge whether it is a packet from LAN to which the packet belongs to which VPN, if a packet is received. Then, a VPN edge router searches the routing table for the VPN concerned, and performs decision of the destination in the network in ISP, and capsulation. Since the VPN edge router holds routing table for every VPN, a VPN edge router cannot mix up a

packet with the same destination IP address received from different VPN, but can transmit it correctly.
[0005] As a method which identifies said VPN, per user circuit interface, VPN-ID for identifying VPN uniquely is assigned, and there is a method which performs VPN discernment by this VPN-ID as indicated by "the Nikkei communication", the October 18, 1999 issue, and p.100, for example. That is, the discernment unit of VPN will be called every physical interface. In this case, even in VPN, one physical interface needs to correspond.
[0006] However, in the aforementioned method, from a company network to the ISP network needs to be connected by one physical circuit. Moreover, only the number of the VPN needs to prepare a physical circuit to connect one company network with two or more VPN. Furthermore, as for a VPN edge router, only the number of VPN to hold needs to hold a physical interface. For this reason, when the number of VPN which a VPN edge router holds becomes large, there is a problem that the number of physical interfaces of a VPN edge router and the number of the routers itself also become large.
[0007] When using an ATM network, a frame relay, etc. which another ISP or the another carrier as an access means to an ISP network which performs a VPN service from a company network offers, since multiplex [ of two or more logical channels ] is carried out into one physical interface, there is also a problem that a physical interface cannot perform VPN discernment at the entry of ISP.
[0008] The purpose of this invention is to enable VPN discernment using the logical channel number multiplexed by the physical interface.
[0009] Moreover, other purposes of this invention are making it possible to perform VPN discernment using the suitable VPN identification information corresponding to each protocol, even when using the protocol with which plurality differs as a lower layer of IP, in case a router holds LAN.
[0010]
[Means for Solving the Problem] In order to solve said technical problem, the VPN edge router of this invention identifies VPN using the channel number for identifying the logical channel multiplexed by the physical interface. As a logical channel number, the information on the lower layer of IP, for example, the information equivalent to the layer 2 specified with the OSI model, is used. When some examples of a logical channel number are given, the lower layer of an IP packet is ATM, and a lower layer is a Frame Relay about header information, such as VPI and VCI, DLCI can be used as a logical channel number. Moreover, when the IP packet is encapsulated by the L2TP header specified by L2TP (Layer2 Tunneling Protocol), the information in a L2TP capsule header (Tunnel ID, session ID, etc.) can be used as a logical channel number. VLAN as which a lower layer is specified by IEEE802.1Q with Ethernet When discernment of VPN is performed using Tag, VLANTag can be used as said logical channel number. When the IP packet is encapsulated for the capsule information specified by the PPP Over Ethernet capsulation method, the capsule information (session ID etc.) specified by the PPP Over Ethernet capsulation method can be used as a logical channel number.
[0011] Furthermore, the VPN identifier setting table for setting the identifier used for VPN discernment as a VPN edge router is prepared. In order that the manager of ISP who manages a VPN edge router may enable it to perform this setup, a user interface is prepared in a VPN edge router. If the case where the lower layer of IP is ATM is explained to an example, when a physical interface will perform VPN discernment, it is set as said VPN identifier setting table with a physical interface. Moreover, in performing VPN discernment by VPI and VCI, it sets it as said VPN identifier setting table with VPI and VCI.
[0012] The interface card unit which holds two or more circuits for which you may carry out as every physical interface, and the protocol same as a lower layer is used is sufficient as the setting unit of a VPN identifier setting table. Moreover, when two or more protocols are multiplexed as a lower layer in one physical interface (for example, circuit by which Time Division Multiplexing of the PPP is carried out to the Frame Relay), the combination of a physical interface and the protocol of the lower layer of IP is sufficient as the setting unit.
[0013] In case ISP holds VPN, actuation of a VPN edge router is concretely explained to an

example for the case where use ATM for the lower layer of IP and VPI and VCI are used as a VPN identifier. A VPN edge router will determine first a VPN identifier (in this example, set up with VPI and VCI), and the VPN discernment table which should be searched according to a setup of a VPN identifier setting table, if a packet is received. In this example, a VPN edge router will search the table in which correspondence with VPI, VCI, and VPN is shown. A VPN edge router judges to which VPN VPI and VCI are used as a search key, a VPN discernment table is searched, and the packet which received belongs. After the judgment is completed, a VPN edge router searches the routing table for VPN to which the packet which received belongs, determines the next destination in an ISP network, and generates capsulation header information used in a network for VPN discernment. A VPN edge router sends out a packet to the next destination which gave and determined header information as the packet.

[0014] Like the above explanation, in order to perform VPN discernment using the logical channel number multiplexed by the physical interface, it is not necessary to prepare a physical interface for a VPN edge router for every VPN by this invention. Moreover, only the number of the VPN does not have the need that only the number of VPN prepares a physical circuit that what is necessary is just to prepare a logical channel to connect one company network with two or more VPN. Moreover, since VPN discernment is performed by the logical channel when using an ATM network, a frame relay, etc. which another ISP or the another carrier as an access means to an ISP network which performs a VPN service from a company network offers, VPN is realizable.

[0015] Furthermore, according to this invention, since a VPN identifier can be chosen for every protocol of the lower layer of IP and the VPN identifier can be set as a VPN identifier setting table, in case the manager of ISP holds VPN, he can use various protocols for a lower layer.

[0016]

[Embodiment of the Invention] Drawing 1 is drawing for explaining one example of VPN constituted using the VPN edge router of this invention. Below, a lower layer shall mean the protocol which encapsulates an IP packet. Moreover, also when you encapsulate an IP packet by IP header, suppose for convenience that this capsule header is written as a header of a lower layer.

[0017] An ISP network (5) has the edge router (9 10) located in a network boundary, and the core router (17) located in a network core. In drawing 1 , although, as for the core router (17), only one is shown, the number is not limited to this. Inside an ISP network (5), capsulation shall be performed by MPLS (based on ATM) and VPN shall be realized. As mentioned above, the method of capsulation is not restricted to this. An ISP network (5) holds LAN1 (1) and LAN2 (2) through an edge router (9), and holds LAN3 (3) and LAN4 (4) through an edge router (10). LAN1 (1) and LAN3 (3) are LANs of the same company A, and constitute VPN among these LANs. Moreover, LAN2 (2) and LAN4 (4) are LANs of the same company B, and constitute VPN also among these LANs. VPN of Company A and Company B will be called VPNA (7) and VPNB (8), respectively.

[0018] An ISP network (5) is logically multiplexed by the circuit (11) through the ATM network (6) which another ISP or an another carrier offers, and LAN1 and LAN2 are connected to the edge router (9). The physical interface of a circuit (11) and an edge router (9) is set to (12). A physical interface is the semantics of the node of a router and a circuit. On the other hand, LAN3 (3) and LAN4 (4) are connected to the edge router (10) through a circuit (13) and (14) using POS (PPP Over SONET) specified by RFC2615, respectively. The physical interface of a circuit (13), (14), and an edge router is set to (15) and (16), respectively.

[0019] In this example, VPI and VCI are used as an identifier which identifies VPN to which LAN1 and LAN2 belong. In the VPN identifier setting table prepared in the edge router (9), it is set to the entry corresponding to a physical interface (12) with VPI and VCI. The number given to the physical interface as an identifier which identifies VPN to which LAN3 and LAN4 belong is used for an edge router (10). In the VPN identifier setting table prepared in the edge router (10), it is set to the entry corresponding to a physical interface (15) and (16) with a physical interface. A VPN identifier setting table is mentioned later.

[0020] Moreover, in the edge router (9), the VPN discernment table showing the correspondence

relation between a VPN identifier and the information (henceforth a VPN number) which shows whether the packet which has the VPN identifier concerned belongs to which VPN is prepared. Above VPNA and VPNB corresponds to a VPN number. Furthermore, in the edge router (9), the routing table showing the relation between a destination IP address and the capsule header information on the method way of an output and an output packet is prepared. The thing for VPNA in this routing table and the thing for VPNB are prepared. It is later mentioned also about a VPN discernment table and routing table.

[0021] An edge router (9) will determine to use VPI and VCI as a VPN identifier according to a setup of a VPN identifier setting table, if the IP packet addressed to LAN3 transmitted from LAN1 is received. After determining a VPN identifier, it judges with an edge router (9) being a packet to which the VPN discernment table in which correspondence with VPI, VCI, and VPN is shown is searched, and the packet concerned belongs to VPNA. Next, an edge router (9) searches the routing table for VPNA by using a destination IP address as a search key, determines the core router (17) of degree the destination, and determines the capsule header of the packet belonging to VPNA for a core router. The packet to which this capsule header was given is transmitted to a core router (17).

[0022] The core router (17) has the routing table showing correspondence relation with degree the destination with a capsule header, i.e., VPI and VCI, uses the capsule header of a receive packet as a search key, determines degree the destination (edge router (10)) and the following capsule header, gives said capsule header, and transmits to an edge router (10).

[0023] An edge router (10) judges that it is the same configuration as an edge router (9), and is the packet which uses the capsule header of a receive packet as a search key, performs VPN discernment like an edge router (9), and belongs to VPNA. Next, the routing table for VPNA is searched by using a destination IP address as a search key, the destination is determined, a capsule header is removed, and a packet is transmitted to LAN3.

[0024] Since an edge router (9) identifies VPN by the logical channel number by which multiplex was carried out to the physical interface and searches the routing table of the VPN concerned, it becomes possible [ identifying VPN by which multiplex was logically carried out to one circuit ]. moreover, the IP address which Company A uses by this -- ** -- even when the IP address which Company B uses carries out batting, the transfer to the right destination is attained.

[0025] Although transmission is performed by the same procedure as the above-mentioned case also when transmitting a packet to LAN2 from LAN4 in VPNB, the edge router (10) which received the IP packet addressed to LAN2 transmitted from LAN4 differs from the case where the point of using a physical interface as a VPN identifier is the above.

[0026] Drawing 2 is drawing for explaining the modification of the example shown in drawing 1 . In this example, LAN1 and LAN2 are directly held in the multiplexer (20) in an ISP network (5) through another circuit (18) and (19). In multiplexer (20), VPNA, different VPI for every VPNB, and VCI are assigned. An edge router (9) performs VPN discernment like the case of drawing 1 using VPI and VCI.

[0027] Drawing 3 is drawing for explaining other modifications of the example shown in drawing 1 .

[0028] LAN5 (21) is added to the network configuration shown in drawing 1 , and VPNB consists of drawing 3 between LAN2, LAN4, and LAN5. LAN5 (21) is connected to the edge router (9) by the circuit (22) using POS. The physical interface of a circuit (22) and an edge router is set to (23).

[0029] VPI and VCI are used for an edge router (9) as an identifier which identifies VPN to which LAN1 and LAN2 belong like explanation of drawing 1 . On the other hand, a physical interface is used for an edge router (9) as an identifier which identifies VPN to which LAN5 belongs. It is set to the VPN identifier setting table in an edge router (9) with a physical interface by the entry corresponding to a physical interface (23). In this example, two kinds of VPN discernment tables of the VPN discernment table in which correspondence with VPI, VCI, and VPN is shown, and the VPN discernment table in which correspondence with a physical interface and VPN is shown are prepared in the edge router (9). The detail is mentioned later.

[0030] For example, when the IP packet addressed to LAN4 transmitted from LAN5 is received,

an edge router (9) determines to use the number of a physical interface as a VPN identifier according to a setup of a VPN identifier setting table. After determining a VPN identifier, an edge router (9) searches the VPN discernment table in which correspondence with a physical interface and VPN is shown by using the number of a physical interface as a search key, and judges that it is the packet to which the IP packet belongs to VPNB. Next, the routing table for VPNB is searched by using a destination IP address as a search key, the core router (17) of degree the destination is determined, and the capsule header of the packet transmitted to the determined core router is determined. This capsule header is given to a packet and it transmits to a core router (17).

[0031] In this example, the VPN identifier was defined for every different underlying protocol, and the VPN discernment table is prepared in each VPN identifier correspondence. By doing in this way, the degree of freedom at the time of corresponding to an underlying protocol which is different with one router increases. That is, if only according to this example it sets up the VPN identifier in a VPN identifier setting table and sets up the VPN discernment table corresponding to the VPN identifier according to the underlying protocol which it is going to hold in an edge router, it becomes possible to hold various underlying protocols in an edge router.

[0032] Next, the detail of the VPN edge router of this invention is explained. When VPN is constituted, a network configuration can consider configurations various besides what was shown in drawing 1 – drawing 3 . Then, it limits to the configuration of the VPN edge router in the case of constituting the network of drawing 1 – drawing 3 , and does not explain, but, more generally the configuration of this invention VPN edge router is explained.

[0033] The example of 1 configuration of a VPN edge router (9) is explained using drawing 8 from drawing 4 . The configuration of a VPN edge router (10) is the same as that of this.

[0034] Drawing 4 is drawing showing the example of 1 configuration of the VPN edge router (9) of this invention. It connects with the lower layer processing section (53 54), the packet layer processing section (52), and a switch (51), and a control section (50) performs control, routing processing, etc. of the whole VPN edge router. The lower layer processing section (53 54) performs termination of the lower layer of IP while holding a circuit (55 56). The packet layer processing section (52) determines the destination of a packet for the information and the IP packet of a lower layer using the information and the header information of an IP packet of reception and its lower layer from the lower layer processing section (53 54). The switch (51) has two or more input/output port, and those ports are connected with the packet layer processing section. A switch (51) consists of crossbar switches. A switch (51) will output the packet to the output port corresponding to the destination of the packet determined in the packet layer processing section (52), if a packet is received from the packet layer processing section (52). A control terminal (57) is connected to said control section (50). The manager of a router is able to perform a setup of the VPN identifier setting table in a router, a VPN discernment table, and routing table etc. with said control terminal. The physical interface numbers 1, 2, 3, and 4 are assigned at the node of the receiving circuit 55-1, 55-2, 55-3 and 55-4, and a router (9), respectively.

[0035] Drawing 5 is drawing showing the example of 1 configuration of the packet layer processing section (52). The lower layer processing section IF (100 106), Switch IF (103 104), and a control section IF (110) are an interface with the lower layer processing section (53 54), an interface with a switch (51), and an interface with a control section (50), respectively. One of the descriptions of this example is in the point of having prepared a VPN identifier setting table (150), a VPN discernment table (151), and the routing table (152) for VPN. These are constituted on memory. These may be constituted on memory physically different, respectively, and may be constituted by the field to which it differs on the same memory. The difference in the method of this configuration is not essential when carrying out this invention. The function and configuration of a block of others which were not explained a VPN identifier setting table (150), a VPN discernment table (151), routing table (152), and here are combined with packet processing actuation of the router (9) explained below, and is explained.

[0036] A packet is received from the circuit (55) which the lower layer processing section (53) has held, the case where a packet is transmitted to the circuit (56) which the lower layer

processing section (54) has held is lengthened for an example, and packet processing of a router (9) is explained.
[0037] The lower layer processing section (53) will carry out termination of the protocol of the lower layer of IP, if a packet is received from LAN. The lower layer processing section (53) transmits the capsule header information on the lower layer used as the physical interface number (it is hereafter called the receiving physics interface number) and the protocol classification of a lower layer which received the packet with the IP packet, and a VPN identifier etc. to the packet layer processing section (52).
[0038] The lower layer processing section interface (100) in the packet layer processing section (52) transmits the capsule header information on the lower layer used as the protocol classification and the VPN identifier of the IP packet transmitted from the lower layer processing section (53), a receiving physics interface number, and a lower layer to the packet transfer processing section (101). The packet transfer processing section (101) extracts IP header information from the IP packet which received, and transmits the capsule header information on the lower layer used as the protocol classification and the VPN identifier of this IP header information, a receiving physics interface number, and a lower layer to VPN discernment and the routing table retrieval processing section (102). An IP packet body is temporarily accumulated into the packet transfer processing section (101).
[0039] VPN discernment and the routing table retrieval processing section (102) search a VPN identifier setting table (150) first by using protocol classification of a receiving physics interface number and a lower layer etc. as a search key, and determines a VPN identifier.
[0040] Drawing 6 shows the example of 1 configuration of a VPN identifier setting table (150). Each entry has a physical interface number (200), a lower layer protocol (203), and a VPN identifier (201). Although the lower layer protocol has established the field of CLP which shows the transfer priority of a packet in the entry of ATM, this field may not exist. The manager of an edge router (9) can set up a VPN identifier from a control terminal (57) as above-mentioned. VPN discernment and the routing table retrieval processing section (102) search using a receiving physics interface number as a search key, and determines a VPN identifier (201). For example, when a receiving physical interface number is 1, a VPN identifier serves as VPI and VCI, and when a receiving physical interface number is 3, a VPN identifier serves as a physical interface number. Like this example, when preparing the CLP field, the combination of VPI, VCI, and CLP and the combination of a physical interface number and CLP may be used as a VPN identifier. About the merit at the time of including CLP (204) in a VPN identifier, it mentions later. When multiplex [ of the packet belonging to two or more VPN ] is carried out logically and it is transmitted to one physical interface, the packet cannot distinguish to which VPN it belongs from a receiving physical interface number. However, if VPI and VCI are used for a VPN identifier when the lower layer is ATM, it will become possible to identify to which VPN the packet belongs. When only the packet belonging to one VPN is transmitted to one physical interface, it is possible to identify VPN by the physical interface number. As a search key, the combination of the protocol (203) of a lower layer and a physical interface number (201) may be used. For example, the circuit connected to the physical interface number 4 is a Time-Division-Multiplexing circuit, and suppose that multiplex [ of the packet which used the Frame Relay for said circuit as a protocol of a lower layer and the packet using a PPP (Point to Point Protocol) protocol ] is carried out. Moreover, to the entry of a Frame Relay, DLCI is set up as a VPN discernment key and a lower layer protocol presupposes that the time slot number is set up for the lower layer protocol as a VPN discernment key to the entry of PPP. In this case, even if it searches only the receiving physical interface number 4 as a search key, it does not become settled uniquely whether a VPN identifier is DLCI or it is a time slot number. Then, a VPN identifier is searched with the combination of a receiving physical interface number and a lower layer protocol in this case.
[0041] If a VPN identifier is determined, VPN discernment and the routing table retrieval processing section will search a VPN discernment table (151) by using the VPN identifier as a search key, and will determine VPN to which the receive packet belongs.
[0042] Drawing 7 (a) and (b) show the example of 1 configuration of a VPN discernment table

(151). Also in which VPN discernment table, each entry has a VPN identifier (201) and a VPN number (250).
[0043] Drawing 7 (a) shows the example of the table which uses VPI and VCI as a VPN identifier (201). It is not necessary to prepare the CLP field (204) of drawing 7 (a), and the priority information field (251) in equipment. The priority information field (251) in equipment are the field which shows the priority information on the packet processing in equipment. According to the VPN identifier determined by retrieval of the aforementioned VPN identifier setting table as a search key, VPN discernment and the routing table retrieval processing section (102) search using the VPN identification information in a packet header as a search key, and determines a VPN number (250). Like this example, when establishing the CLP field (204) and the priority information field (251) in equipment in a VPN discernment table (151), as a search key, the combination of CLP (204), VPI, and VCI which shows the transfer priority of a packet may be used. By including CLP in a search key, different priority information in equipment can be defined to the packet belonging to the same VPN number. For example, "VPI, VCI=a" and in the case of "CLP=0", "priority in equipment =a", "VPI, VCI=a", and in the case of "CLP=1", priority information in equipment which is different to the packet belonging to the same VPN number as shown in "priority in equipment =b" can be defined.
[0044] Drawing 7 (b) shows the example of the table which uses a physical interface number (252) as a VPN identifier (201). If the priority control of packet processing is not performed, it is not necessary to prepare the priority information field (251) in equipment of drawing 7 (b).
[0045] What is necessary is just to constitute the same table as drawing 7 (a) and (b), when VPN identifiers other than the above, for example, DLCI, a time slot number, etc. are used. That is, a VPN discernment table (151) is prepared for every VPN identifier, and these setup is set up from a control terminal (54). The VPN discernment table (151) prepared for every VPN identifier may be constituted on the same memory, and may be constituted on different memory, respectively.
[0046] If a VPN number is determined, VPN discernment and the routing table retrieval processing section will search the routing table (152) for VPN corresponding to the VPN number, and will determine the output capsule header information for VPN added to the packet belonging to the method way of an output, and its VPN number.
[0047] Drawing 8 shows the example of 1 configuration of the routing table (152) for VPN. VPN discernment and the routing table retrieval processing section (102) hold this routing table (152) for VPN for every VPN to hold. The routing table (152) for VPN prepared for every VPN of this may be constituted on the same memory, and may be constituted on memory different, respectively. The routing table (152) for VPN has a destination IP address (300), a method way number (301) of an output, and output capsule header information (302). The method way number (301) of an output is an identifier in equipment for transmitting a packet to a desired interface with a switch etc. Output capsule header information (302) is the capsule header information that it uses in an ISP network (5). VPN discernment and the routing table retrieval processing section (102) search routing table for VPN corresponding to the VPN number (250) determined by retrieval of the aforementioned VPN discernment table, using the destination IP address in IP header as a search key, and determines the method way number (301) of an output, and output capsule header information (302). In this example, since the routing table (152) for VPN is prepared for every VPN, even if the same IP address is used in two or more VPN, the method way of a right output can be determined.
[0048] If the method way number (301) of an output and output capsule header information (302) are determined, VPN discernment and the routing table retrieval processing section (102) will transmit the method way (301) of an output and output capsule header information (302) which were determined to the packet transfer processing section (101).
[0049] The packet transfer processing section (101) transmits the IP packet body which was being accumulated, the method way number (301) of an output, and output capsule header information (302) to a switch (51) through Switch IF (103). A switch (51) outputs the IP packet body received from the packet transfer processing section (101), and its output capsule header information (302) to the output port corresponding to the method way number of an output.
[0050] The packet layer processing section (52) of the side which receives the IP packet body

transmitted from the packet layer processing section connected to the above-mentioned output port (52), i.e., the packet layer processing section, (52) and its output capsule header information (302) receives them through Switch IF (104). If an IP packet body and its output capsule header information (302) are received, the packet transfer processing section (105) will transmit these to the lower layer processing section (54) through the lower layer processing section IF (106). If an IP packet body and its output capsule header information (302) are received, the lower layer processing section (54) will generate a capsule header based on the output capsule header information, and will encapsulate an IP packet body by the capsule header, and will transmit the encapsulated packet to a core router (17).

[0051] In the above, the example of 1 configuration of VPN edge router equipment was explained using drawing 8 from drawing 4 . Even if it is the case where the packet belonging to different VPN is transmitted to the same physical interface by using the router equipment of this example, it becomes possible to identify VPN to which they belong. Moreover, since the suitable VPN identifier corresponding to each underlying protocol can be set as a VPN identifier setting table even when the same edge router holds two or more LANs which use the underlying protocol of different IP, the degree of freedom of VPN construction increases.

[0052] Although the direct output of the output capsule header information is carried out as a retrieval result of the routing table for VPN, you may make it output an output capsule number in this example. This output capsule number is an identifier in equipment for giving a capsule header in the lower layer processing section of an output side. In this case, the header generation table which made the capsule number and the capsule header the pair is prepared in the lower layer processing section of an output side. The lower layer processing section of an output side searches a header generation table using a search key and a **** capsule number, and determines a capsule header.

[0053] The table shown by this example is a logical table, may use the retrieval algorithm represented by the tree structure as a table search method, and may adopt the configuration using CAM (Content Addressable Memory), and the method which carries out the sequential retrieval of the table.

[0054] When VPN edge router equipment holds a Time-Division-Multiplexing circuit, the lower layer processing section may apply a time slot number besides [ which was explained by this example ] each information as information transmitted to the packet layer processing section. In this case, a time slot number may be set as a VPN identifier setting table as a VPN identifier. Moreover, a time slot number may be used as a search key of a VPN discernment table.

[0055] VLAN besides [ which was explained by this example as information which the lower layer processing section transmits to the packet layer processing section when VPN edge router equipment held Ethernet and VLAN capsulation of the packet on Ethernet was carried out according to IEEE802.1Q ] each information Tag information may be added. In this case, it is VLAN to a VPN identifier setting table as a VPN identifier. Tag information may be set up. Moreover, it is VLAN as a search key of a VPN discernment table. Tag information may be used.

[0056] When the IP packet is encapsulated by the L2TP header specified by L2TP (Layer2 Tunneling Protocol), each information in a L2TP capsule header (Tunnel ID, session ID, etc.) may be set as a VPN identifier setting table as a VPN identifier.

[0057] Moreover, when the IP packet is encapsulated for the capsule information specified by the PPP Over Ethernet capsulation method, the lower layer processing section may add the capsule information specified as information transmitted to the packet layer processing section by the PPP Over Ethernet capsulation method besides [ which was explained by this example ] each information. In this case, the capsule information (session ID etc.) specified on the VPN identifier setting table by the PPP Over Ethernet capsulation method may be set up as a VPN identifier.

[0058] Drawing 9 shows other examples of a configuration of the VPN edge router equipment (9) of this invention. An interface card (400 401) is a card which holds the circuit using the protocol of the same low order layer, respectively. For example, an interface card (400) is an interface card for ATM, and holds an ATM circuit (402). Moreover, an interface card (401) is an interface card for POS, and holds a POS circuit (403). The interface card (400 401) is removable and, as

for the manager of a router, only required quantity can carry the required interface card for low order layer protocols. The lower layer processing section (405 406) which performs processing peculiar to each lower layer protocol is carried in each interface card. Actuation of the lower layer processing section (405 406) is the same as that of the lower layer processing section (53 54) of drawing 4 . A packet processing card (407) is a card which performs reception and packet layer processing for information, such as an IP packet, from said interface card. Each packet processing card (407) is removable, and, as for the manager of a router, only required quantity can carry it. The packet layer processing section (52) explained using drawing 4 and drawing 5 is carried in each packet processing card (407). A manager can set up flexibly the configuration of the VPN identifier setting table in a packet processing card (407), a VPN discernment table, and the routing table for VPN from a control terminal (57) according to the classification of the interface card to hold, and the configuration of the access network between LAN and an interface card. Packet processing actuation of the VPN edge router equipment of this example is the same as the actuation explained using drawing 8 from drawing 4 .

[0059] Drawing 10 to drawing 12 is drawing showing the relation between the interface card held in the packet processing card (407) of drawing 9 , and the VPN identifier setting table held at a packet processing card, a VPN discernment table and the routing table for VPN. Drawing 12 indicates only an interface card and a packet processing card to be LANs held in an edge router among the components of an edge router (9) from drawing 10 . Moreover, the VPN identifier setting table in a packet processing card, a VPN discernment table, and the routing table for VPN are logical. Drawing 12 shows the case where the same VPN identifier is used, from drawing 10 to all the physical interfaces in the same interface card. For this reason, since it is not necessary to set up a physical interface number as a search key of a VPN identifier setting table, by drawing 12 , the physical interface number as that search key is omitted from drawing 10 . What is necessary is just to use a physical interface as a search key of a VPN identifier setting table as mentioned above, when a different VPN identifier is used within the same interface card.

[0060] Drawing 10 shows the example of 1 configuration of the VPN identifier setting table in a packet processing card in case the interface card (400) for ATM is held, a VPN discernment table, and the routing table for VPN to a packet processing card (407). LAN1 (450) belongs to VPNA and presupposes that LAN2 (451) is belonged to VPNB. Multiplex [ of the packet from LAN1 and LAN2 ] is carried out with multiplexer (452), and it is held in the interface card (400) for ATM through a circuit (453). In case multiplex is carried out, suppose that the value a and b is assigned to the packet as VPI and a VCI from LAN1 and LAN2, respectively. VPI and VCI are used for VPN discernment in this example. VPI and VCI are set to the VPN identifier setting table (455) in a packet processing card (407) as a VPN identifier. VPI and VCI are set to a VPN discernment table (456) as a search key. As routing table for VPN, the routing table (457) for VPNA and the routing table (458) for VPNB are prepared. For example, if a packet is received from LAN1, the lower layer processing section (405) in the interface card (400) for ATM will carry out termination of the ATM protocol, and will transmit an IP packet body and VPI and VCI, a physical interface number, etc. to a packet processing card (407). The VPN discernment and the routing table retrieval processing section in a packet processing card (407) search a VPN identifier setting table (455), and determines to use VPI and VCI as a VPN identifier. Next, a VPN discernment table (456) is searched using VPI of a receive packet, the value of VCI, and "a", and it judges that a receive packet belongs to VPNA. Next, the routing table (457) for VPNA is searched and the method way of an output and output capsule header information are determined.

[0061] Drawing 11 shows the example of 1 configuration of the VPN identifier setting table in a packet processing card in case the interface card (401) for POS is held, a VPN discernment table, and the routing table for VPN to a packet processing card (407).

[0062] LAN1 (450) belongs to VPNA and presupposes that LAN2 (451) is belonged to VPNB. LAN1 and LAN2 are held in the interface card (401) for POS through a circuit (500) and (501), respectively. The physical interface number of a circuit (500) and a circuit (501), and the interface card (401) for POS is set to 1 and 2, respectively. In this case, in order to use a

physical interface for VPN discernment, a physical interface number is set to the VPN identifier setting table (455) in a packet processing card (407) as a VPN identifier. A physical interface number is set to a VPN discernment table (456) as a search key. As routing table for VPN, the routing table (457) for VPNA and the routing table (458) for VPNB are prepared. The processing in a packet processing card (407) is the same as the processing explained using drawing 10 . However, the points using VPI and not VCI but a physical interface as a VPN identifier differ.

[0063] Although drawing 12 is not illustrated to drawing 9 , it shows the example of 1 configuration of the VPN identifier setting table in a packet processing card in case the interface card (550) for Time-Division-Multiplexing circuits is held, a VPN discernment table, and the routing table for VPN to a packet processing card (407). LAN1 (450), LAN2 (451), and LAN3(551) LAN4 (552) presuppose that it belongs to VPNA, VPNB, VPNC, and VPND, respectively. The underlying protocol of LAN1 and LAN2 is made into a Frame Relay, and the underlying protocol of LAN3 and LAN4 is set to PPP (Point to Point Protocol). 10 and 20 are assigned to a packet as DLCI from LAN1 and LAN2, respectively, and those packets are multiplexed by the circuit (554) in Frame Relay multiplexer (553). Furthermore, in a time division multiplexer (555), multiplex [ of a circuit (554), (556), and (557) ] is carried out to a circuit (558). Under the present circumstances, suppose that time slot numbers 1, 2, and 3 are assigned to the data of a circuit (554), (556), and (557), respectively. Suppose that DLCI is used as a VPN identifier to LAN1 and LAN2, and a time slot number is used as a VPN identifier to LAN3 and LAN4. In this case, to the entry whose lower layer protocol (559) in a VPN identifier setting table (455) is a Frame Relay, DLCI (560) is set up as a VPN identifier. Moreover, to the entry whose lower layer is PPP, a time slot number (561) is set up as a VPN identifier. As a VPN discernment table, two tables (562), i.e., the VPN discernment table showing correspondence of DLCI and a VPN number, and the VPN discernment table (563) showing correspondence of a time slot number and a VPN number are prepared. Moreover, the routing table (457) for VPNA, the routing table (458) for VPNB, the routing table (564) for VPNC, and the routing table (565) for VPND are prepared as routing table for VPN. The processing in a packet processing card (407) is the same as the processing explained using drawing 10 . However, it differs in that a lower layer protocol (559) is used as a search key at the time of VPN identifier setting table retrieval. Moreover, it differs in that DLCI is used as a VPN identifier about the packet which received from LAN1 and LAN2, and a time slot number is used about the packet which received from LAN3 and LAN4 as a result of VPN identifier setting table retrieval.

[0064] Although the example in which one packet processing card holds one interface card in drawing 12 was explained from drawing 9 , a packet processing card is very good in the configuration which holds two or more interface cards. You may be [ from which two or more interface cards to hold differ in that case ] for underlying protocols.

[0065] Drawing 13 shows the example of 1 configuration of the VPN identifier setting table in a packet processing card in case an interface card for underlying protocols which is different on a packet processing card (407) is held, a VPN discernment table, and the routing table for VPN. An interface card (400) and (401) carry out to the object for ATM, and POS, respectively. Drawing 13 shows the case where a VPN identifier is the same, to all the physical interfaces in the same interface card. It is ****** by which the ******** card numbers 1 and 2 are assigned to each interface card (400) and (401) in order that a packet transfer card may hold two or more interface cards by this example. Moreover, a card number (602) is set up as a search key of a VPN identifier setting table (455). LAN1 (450), LAN2 (451), and LAN3(551) LAN4 (552) presuppose that it belongs to VPNA, VPNB, VPNC, and VPND, respectively. Multiplex [ of the packet from LAN1 and LAN2 ] is carried out with multiplexer (452), and it is held in the interface card (400) for ATM through a circuit (453). In case multiplex is carried out, the value a and b shall be assigned to a packet as VPI and a VCI from LAN1 and LAN2, respectively. In this case, what is necessary is just to use VPI and VCI for VPN discernment. To the entry (603) of a card number 1 in a VPN identifier setting table (455), VPI and VCI are set up as a VPN identifier. LAN3 and LAN4 are held in the interface card (401) for POS through a circuit (500) and (501), respectively. The physical interface number of a circuit (500), and a (501) and the interface card (401) for POS is set to 1 and 2, respectively. In this case, what is necessary is just to use a

physical interface for VPN discernment. To the entry (604) of a card number 2 in a VPN identifier setting table (455), a physical interface is set up as a VPN identifier. As a VPN discernment table, the table (600) showing correspondence of VPI, VCI, and a VPN number and the table (601) showing correspondence of a physical interface number and a VPN number are prepared. As routing table for VPN, the routing table (457) for VPNA, the routing table (458) for VPNB, the routing table (564) for VPNC, and the routing table (565) for VPND are prepared. The processing in a packet processing card (407) is the same as the processing explained using drawing 10 . However, it differs in that a card number (602) is used as a search key at the time of VPN identifier setting table retrieval. Here, although the case where ATM and POS were held was shown, it is not restricted to this combination. For example, it is also possible to change the interface card for POS to the interface card for FR. In this case, you may make it the packet from LAN3 and LAN4 identify VPN by DLCI so that multiplex may be carried out to one circuit and it may be inputted into the interface card for FR like LAN1 and LAN2.

[0066] As mentioned above, as explained using drawing 13 from drawing 9 , according to the router equipment of this example, a manager can set up flexibly the configuration of the VPN identifier setting table in a packet processing card (407), a VPN discernment table, and the routing table for VPN from a control terminal (57) according to the classification of the interface card to hold. Moreover, since VPN is identified by the logical channel number by which multiplex was carried out to the physical interface, it becomes possible to identify VPN by which multiplex was logically carried out to one circuit.

[0067] An example of the configuration procedure of a packet processing card (407) at the time of equipping drawing 14 with an interface card is shown. After a VPN edge router (9) is equipped with an interface card, the VPN identifier setting table (455) in a packet processing card (407) is set up (701 702). A manager can set up a setup of a VPN identifier setting table freely by classification of the interface card with which it equips. Next, a VPN discernment table is set up for every set-up VPN identifier (703). Routing table is set up for every VPN (704).

[0068] In case a setup of a VPN identifier equips a packet processing card with an interface card, it communicates between an interface card and a packet processing card, judges automatically the protocol of the lower layer of the IP packet in which an interface card carries out termination, and you may make it notify it to a packet processing card. The identification information specified corresponding to the protocol of the notified lower layer can be set automatically on a VPN identifier setting table.

[0069] In the above, actuation of the VPN edge router of this invention was explained using drawing 1 - drawing 14 . The flow of operation common to these is shown in drawing 15 .

[0070] If the packet which encapsulated the IP packet from LAN is received (801), a VPN edge router will search a VPN identifier setting table (802), and will determine the VPN identifier of a receive packet (803). As a VPN identifier, although logical channel identifiers, such as VPI and VCI, are used, according to the underlying protocol to hold, you may use it combining this, a physical interface number, etc. Next, a VPN discernment table is searched by using the determined VPN identifier as a search key (804), and VPN to which a receive packet belongs is determined (805). For example, when VPN identifiers are VPI and VCI, a VPN discernment table is searched by using as a search key VPI and VCI which were assigned to the receive packet, and VPN to which a receive packet belongs is determined. The determined routing table for VPN is searched (806), and the method way of an output and the capsule header for an output are determined (807).

[0071]

[Effect of the Invention] By using the router of this invention, VPN is discriminable using the logical channel number multiplexed by the physical interface. Therefore, the number of VPN to hold can be increased, without increasing a physical circuit.

[0072] Moreover, since the suitable VPN identifier corresponding to each protocol can be set up even when two or more LANs which a router holds use the underlying protocol of IP different, respectively, VPN discernment can be performed.

[Translation done.]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing for explaining one example of VPN constituted using the VPN edge router of this invention.
[Drawing 2] It is drawing for explaining the modification of the example shown in drawing 1 .
[Drawing 3] It is drawing for explaining other modifications of the example shown in drawing 1 .
[Drawing 4] It is drawing showing the example of 1 configuration of the VPN edge router of this invention.
[Drawing 5] It is drawing showing the example of 1 configuration of the packet layer processing section.
[Drawing 6] It is drawing showing the example of 1 configuration of a VPN identifier setting table (150).
[Drawing 7] It is drawing showing the example of 1 configuration of a VPN discernment table.
[Drawing 8] It is drawing showing the example of 1 configuration of the routing table for VPN.
[Drawing 9] It is drawing showing other examples of a configuration of the VPN edge router equipment of this invention.
[Drawing 10] It is drawing showing the example of 1 configuration of the VPN identifier setting table in a packet processing card in case the interface card for ATM is held, a VPN discernment table, and the routing table for VPN on a packet processing card.
[Drawing 11] It is drawing showing the example of 1 configuration of the VPN identifier setting table in a packet processing card in case the interface card for POS is held, a VPN discernment table, and the routing table for VPN on a packet processing card.
[Drawing 12] It is drawing showing the example of 1 configuration of the VPN identifier setting table in a packet processing card in case the interface card for Time-Division-Multiplexing circuits is held, a VPN discernment table, and the routing table for VPN on a packet processing card.
[Drawing 13] It is drawing showing the example of 1 configuration of the VPN identifier setting table in a packet processing card in case an interface card for underlying protocols which is different on a packet processing card is held, a VPN discernment table, and the routing table for VPN.
[Drawing 14] It is drawing showing an example of the configuration procedure of a packet processing card.
[Drawing 15] It is the flow chart which shows the flow of the VPN edge router of this invention of operation.
[Description of Notations]
5 [ — A switch, 52 / — 53 The packet layer processing section 54 / — 101 The lower layer processing section 105 / — The packet transfer processing section 102 / — VPN discernment and the routing table retrieval processing section, 150 / — A VPN identifier setting table 151 / — A VPN discernment table, 152 / — Routing table, 400 / — The interface card for ATM, 401 / — The interface card for POS, 407 / — Packet processing card. ] — An ISP network, 9 — A VPN edge router, 50 — A control section, 51

[Translation done.]

* NOTICES *

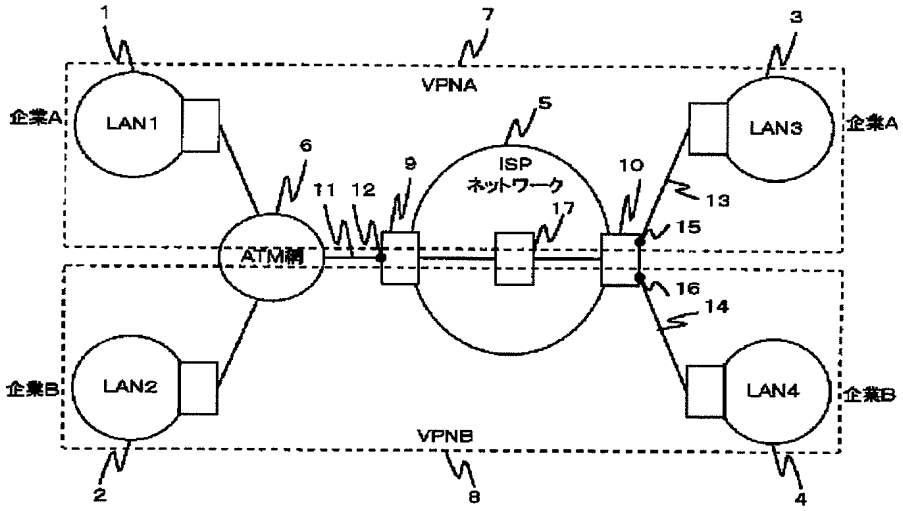


1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DRAWINGS

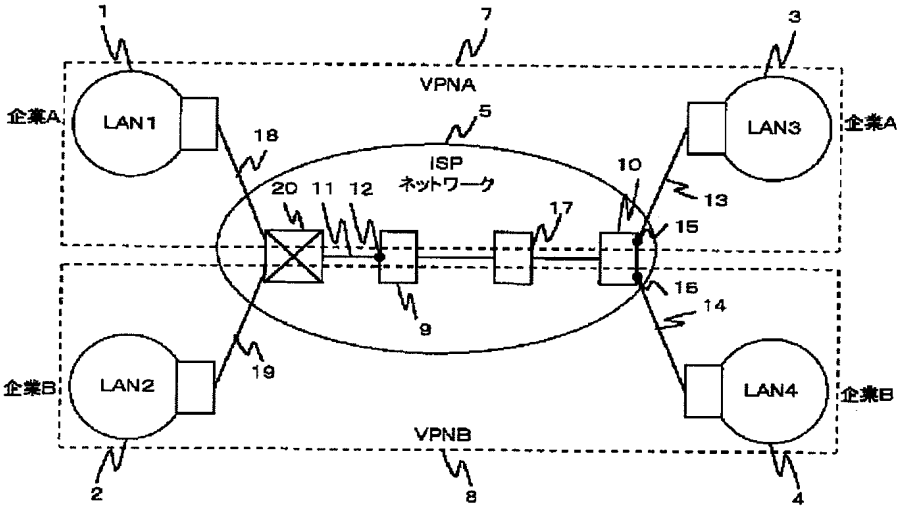
[Drawing 1]

図1



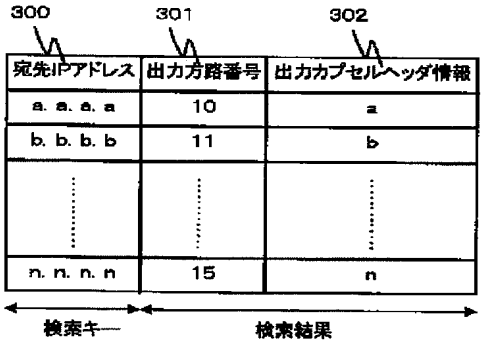

[Drawing 2]

図2



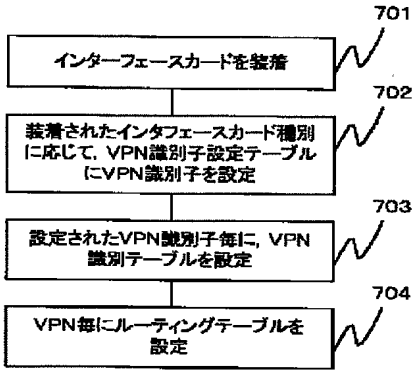

[Drawing 8]

図8



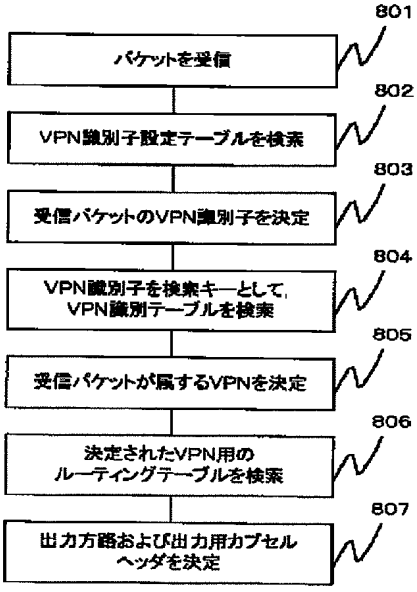

[Drawing 14]

図14



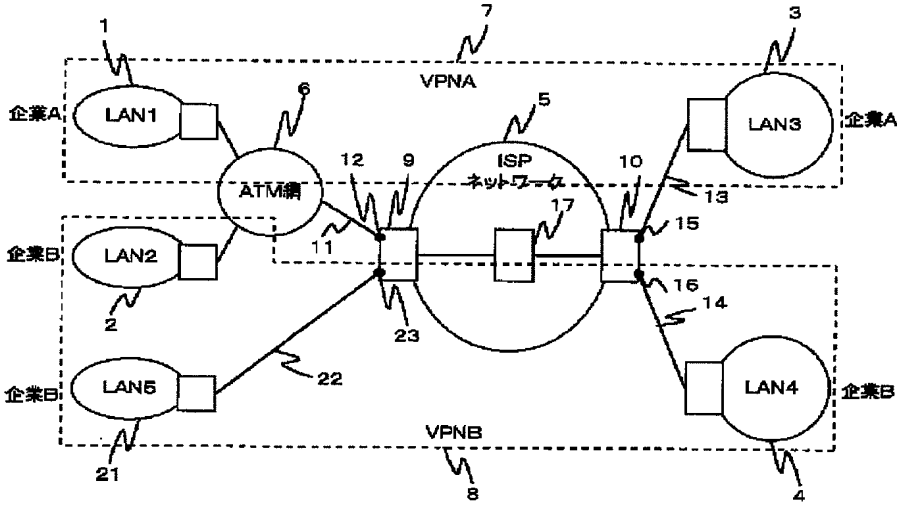

[Drawing 15]

図15



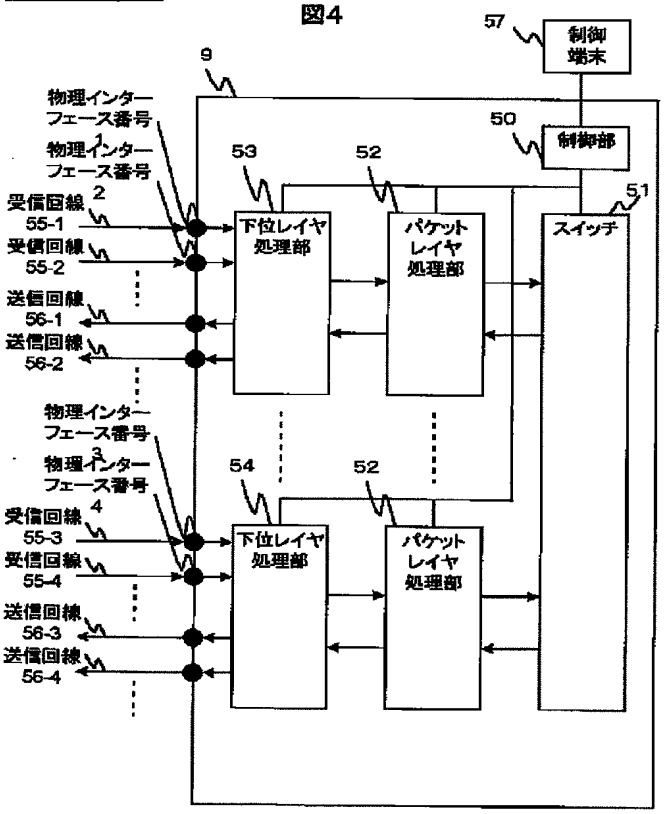

[Drawing 3]

図3



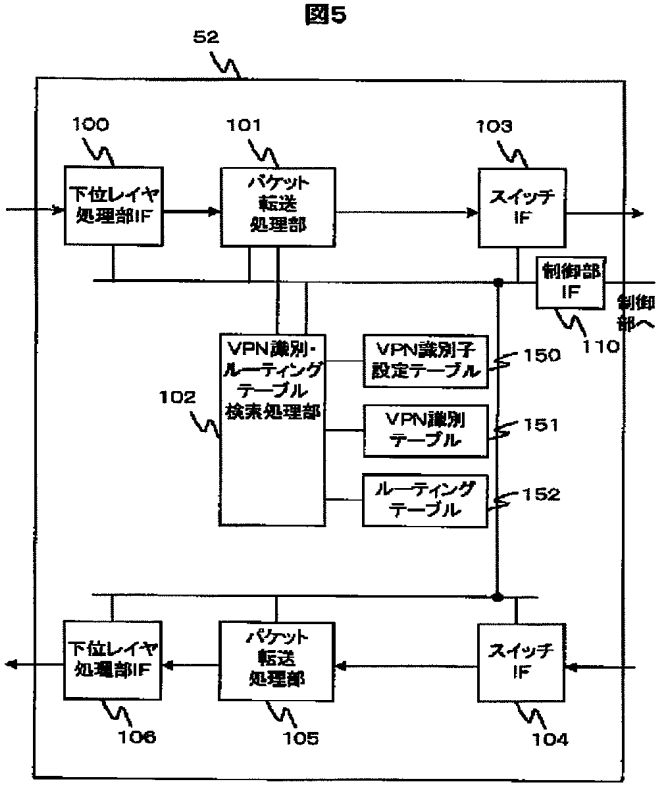

[Drawing 4]

図4



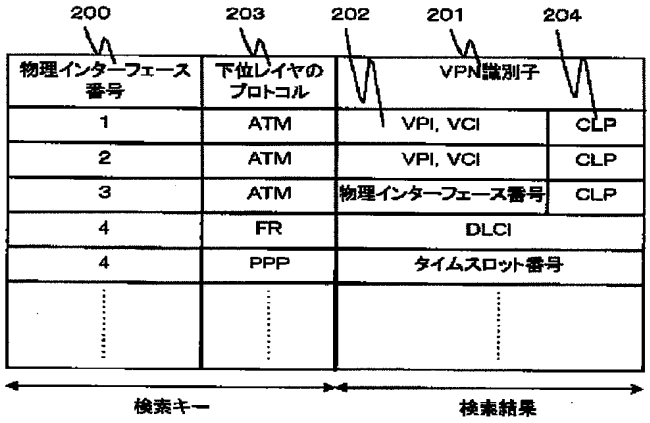

[Drawing 5]

図5




[Drawing 6]

図6




[Drawing 7]

図7

(a)

| 202 | 201 | 204 | 250 | 251 |
|---|---|---|---|---|
| VPN識別子 | | | VPN番号 | |
| VPI, VCI | CLP | | VPN番号 | 装置内優先度情報 |
| a | 0 | | VPNA | a |
| a | 1 | | VPNA | b |
| b | 0 | | VPNB | c |
| b | 1 | | VPNB | d |
| ⋮ | ⋮ | | ⋮ | ⋮ |

検索キー　　検索結果

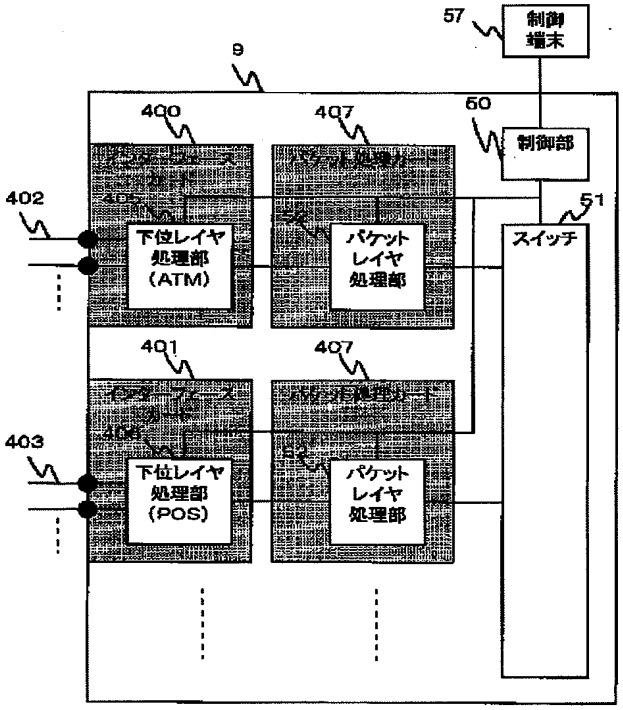
(b)

| 252 | 201 | 250 | 251 |
|---|---|---|---|
| VPN識別子 | | VPN番号 | |
| 物理インターフェース番号 | | VPN番号 | 装置内優先度情報 |
| 3 | | VPNA | a |
| ⋮ | | ⋮ | ⋮ |
| n | | VPNB | b |
| ⋮ | | ⋮ | ⋮ |

検索キー　　検索結果

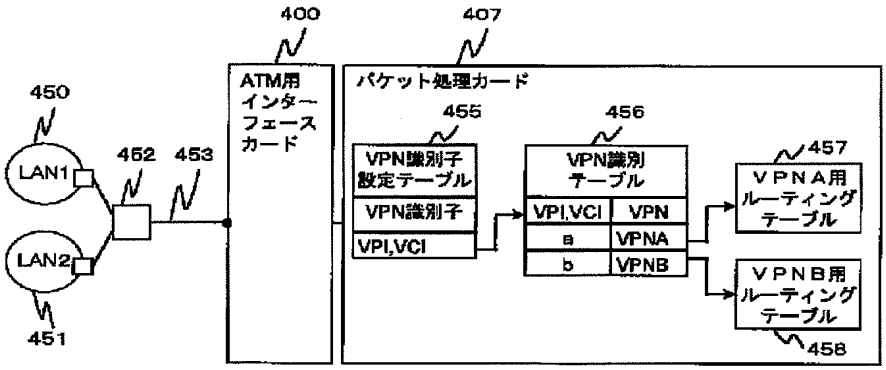
[Drawing 9]

図9



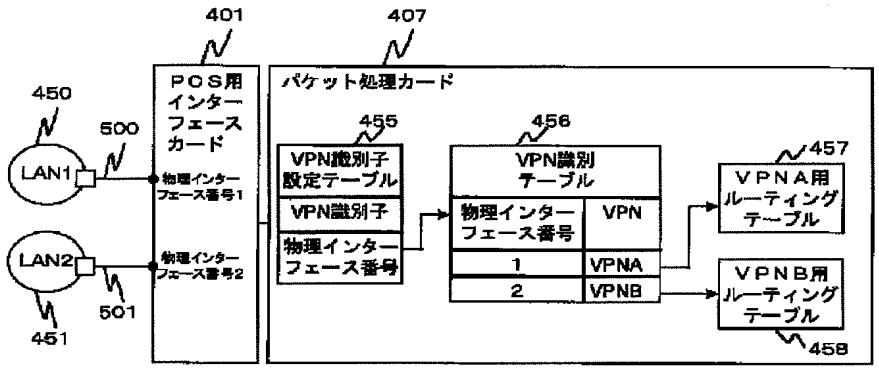

[Drawing 10]

図10



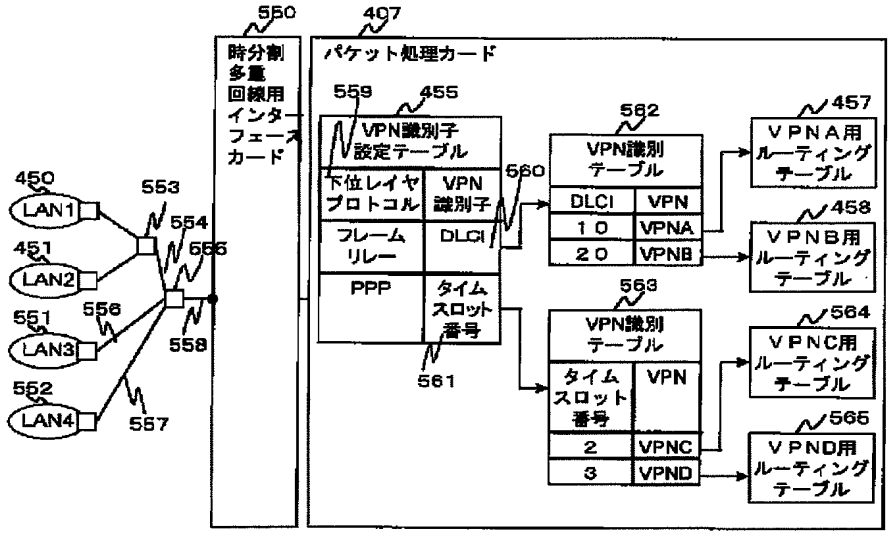

[Drawing 11]

図11



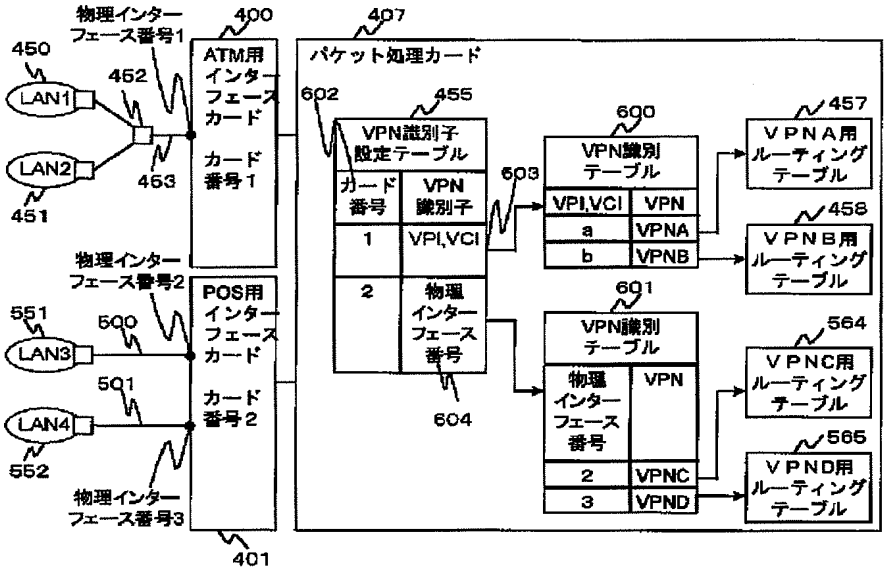

[Drawing 12]

図12




[Drawing 13]

図13




[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－345864
（P2001－345864A）
(43)公開日　平成13年12月14日(2001.12.14)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ　12/66 | | Ｈ０４Ｌ　11/20 | Ｂ | ５Ｋ０３０ |
| 12/46 | | 11/00 | ３１０Ｃ | ５Ｋ０３３ |
| 12/28 | | 11/20 | Ｇ | |
| 12/56 | | | １０２Ｄ | |

審査請求　未請求　請求項の数23　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－170414(P2000－170414)
(22)出願日　平成12年６月２日(2000.6.2)

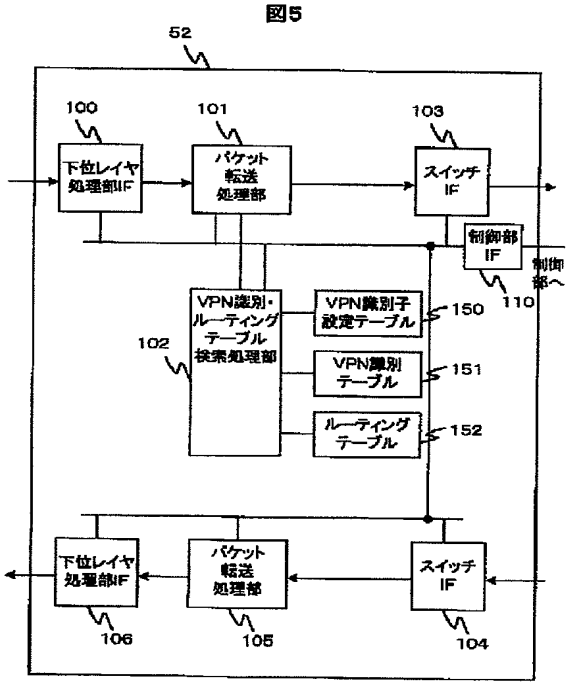
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　赤羽　真一
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　坂本　健一
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ルータ装置，パケット転送制御方法及びＶＰＮ識別情報の設定方法

(57)【要約】
【課題】　同一回線に複数のＶＰＮ（Virtual Private Network）が多重される場合に、この回線を収容するエッジルータにおいて、受信したパケットが何れのＶＰＮに属するかを識別する手段を提供することである。
【解決手段】　ＶＰＮエッジルータに、同一回線に多重化されている論理的なチャネル番号を用いてＶＰＮを識別する機能を設ける。
【効果】　物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮを識別することができる。従って、物理回線を増やすことなく、収容するＶＰＮの数を増やすことができる。

図5



1

【特許請求の範囲】

【請求項１】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容することができるルータ装置であって、

複数の論理チャネルが多重された受信回線を収容する物理インタフェースと、上記複数の論理チャネルの各論理的なチャネルに割り当てられている論理チャネル識別子と、上記複数のＶＰＮに割り当てられているＶＰＮ名との対応関係を示すテーブルを保持するメモリと、

上記複数の論理チャネルのうちの一つの論理チャネルを介して送信されたパケットを受信した際、上記論理チャネルに割り当てられている論理チャネル識別子を検索キーとして上記テーブルを検索し、上記受信パケットが上記複数のＶＰＮのうち何れのＶＰＮに属するかを判断する処理部、とを有することを特徴とするルータ装置。

【請求項２】請求項１に記載のルータ装置であって、

それぞれ、送信回線が収容される複数の物理インタフェースと、

上記複数のＶＰＮの各ＶＰＮ対応に、各ＶＰＮで使用されるパケットのアドレス情報と、上記複数の物理インタフェースを識別する情報との対応関係を示すルーティングテーブルを保持するメモリ、とを有し、

上記処理部は、上記パケットのヘッダ部に格納される宛先アドレス情報を検索キーとして上記ルーティングテーブルを検索し、上記複数の物理インタフェースのうち何れの物理インタフェースから上記受信パケットを送信するかを決定することを特徴とするルータ装置。

【請求項３】請求項２に記載のルータ装置であって、

上記ルーティングテーブルは、各ＶＰＮで使用されるパケットのアドレス情報と、パケットを出力する際に付与するヘッダ情報との関係を保持し、

上記処理部は、上記パケットのヘッダ部に格納される宛先アドレス情報を検索キーとして上記ルーティングテーブルを検索し、上記受信パケットに付与するパケットヘッダ情報を決定することを特徴とするルータ装置。

【請求項４】請求項２又は請求項３の何れかに記載のルータ装置であって、

上記テーブルと上記ルーティングテーブルとは物理的に同一のメモリ上に保持されることを特徴とするルータ装置。

【請求項５】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、非同期転送モード（ＡＴＭ）回線であり、上記論理チャネル識別子は、ＶＰＩ及びＶＣＩであることを特徴とするルータ装置。

【請求項６】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、フレームリレー回線であり、上記論理チャネル識別子は、ＤＬＣＩであることを特徴とするルータ装置。

2

【請求項７】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、Ｌ２ＴＰ（Layer2 Tunneling Protocol）で規定されているＬ２ＴＰヘッダでカプセル化されたパケットが送信され、上記論理チャネル識別子は、Ｌ２ＴＰカプセルヘッダ内の情報であることを特徴とするルータ装置。

【請求項８】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、イーサネット（登録商標）回線であり、上記論理チャネル識別子は、IEEE802.1Qで規定されるＶＬＡＮ　Ｔａｇであることを特徴とするルータ装置。

【請求項９】請求項１乃至請求項４の何れかに記載のルータ装置であって、

上記受信回線は、ＰＰＰ　Ｏｖｅｒ　Ｅｔｈｅｒｎｅｔ（登録商標）でカプセル化されたパケットが送信され、上記論理チャネル識別子は、そのカプセルヘッダ内の情報であることを特徴とするルータ装置。

【請求項１０】請求項１乃至請求項９の何れかに記載のルータ装置であって、

上記ルータ装置は、制御端末と接続することが可能であり、

上記制御端末から、上記テーブル内に保持される上記論理チャネル識別子と、上記ＶＰＮ名との対応関係を設定することができることを特徴とするルータ装置。

【請求項１１】ルータ装置であって、

第１のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する第１のローカル・エリア・ネットワーク（以下「ＬＡＮ」という。）及び第２のＶＰＮに属する第２のＬＡＮから同一のプロトコルでカプセル化されたパケットが多重されて送信される回線を収容するインタフェース部と、

上記第１の回線から受信したパケットが上記第１のＶＰＮに属するのか、上記第２のＶＰＮに属するのかを識別するための識別子を設定する手段、とを有することを特徴とするルータ装置。

【請求項１２】請求項１１に記載のルータ装置であって、

上記プロトコルは非同期転送モードプロトコルであり、上記識別子はＶＰＩ及びＶＣＩであることを特徴とするルータ装置。

【請求項１３】ルータ装置であって、

それぞれ、異なるバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する複数のローカル・エリア・ネットワーク（以下「ＬＡＮ」という。）から第１のプロトコルでカプセル化されたパケットが送信される第１の回線を収容する第１のインタフェース部と、

それぞれ、異なるＶＰＮに属するＶＰＮに属する複数の

ＬＡＮから第２のプロトコルでカプセル化されたパケットが送信される第２の回線を収容する第２のインタフェース部と、
上記第１の回線から受信したパケットが何れのＶＰＮに属するのかを識別するための第１の識別子を設定する手段と、
上記第２の回線から受信したパケットが何れのＶＰＮに属するのかを識別するための第２の識別子を設定する手段とを有し、
上記第２の識別子は上記第１の識別子とは異なることを特徴とするルータ装置。
【請求項１４】請求項１３に記載のルータ装置であって、
上記第１のプロトコルは非同期転送モードプロトコルであり、上記第１の識別子はＶＰＩ及びＶＣＩであり、
上記第２のプロトコルはフレームリレーであり、上記第２の識別子はＤＬＣＩであることを特徴とするルータ装置。
【請求項１５】ルータ装置であって、
第１のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する第１のローカル・エリア・ネットワーク（以下「ＬＡＮ」という。）から第１のプロトコルでカプセル化されたパケットと、第２のＶＰＮに属する第２のＬＡＮから上記第１のプロトコルでカプセル化されたパケットととが多重されて送信される第１の回線を収容する第１のインタフェース部と、
第３のＶＰＮに属する第３のＬＡＮから第２のプロトコルでカプセル化されたパケットが送信される第２の回線と、第４のＶＰＮに属する第４のＬＡＮから上記第２のプロトコルでカプセル化されたパケットが送信される第３の回線とを収容する第２のインタフェース部と、
上記第１の回線から受信したパケットが上記第１のＶＰＮに属するのか、上記第２のＶＰＮに属するのかを識別するための第１の識別子を設定する手段と、
上記第２の回線及び上記第３の回線から受信したパケットが上記第３のＶＰＮに属するのか、上記第４のＶＰＮに属するのかを識別するための第２の識別子を設定する手段、
とを有し、
上記第２の識別子は上記第１の識別子とは異なることを特徴とするルータ装置。
【請求項１６】請求項１５に記載のルータ装置であって、
上記第１のプロトコルは非同期転送モードプロトコルであり、上記第１の識別子はＶＰＩ及びＶＣＩであり、
上記第２のプロトコルはＰＰＰ over ＳＯＮＥＴであり、上記第２の識別子は、上記第３の回線と上記第４の回線とを識別するための物理インタフェース番号であることを特徴とするルータ装置。
【請求項１７】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容することができるルータ装置におけるパケット転送制御方法であって、上記ルータ装置は、複数の論理チャネルが多重された受信回線を収容し、上記複数の論理チャネルの各論理的なチャネルに割り当てられている論理チャネル識別子と、上記複数のＶＰＮに割り当てられているＶＰＮ名との対応関係を示すテーブルを有し、
上記方法は、
上記複数の論理チャネルのうちの一つの論理チャネルを介して送信されたパケットを受信し、
上記論理チャネルに割り当てられている論理チャネル識別子を検索キーとして上記テーブルを検索し、
上記受信パケットが上記複数のＶＰＮのうち何れのＶＰＮに属するかを判断する、ステップを有することを特徴とする。
【請求項１８】請求項１７に記載のパケット転送制御方法であって、
上記受信回線は、非同期転送モード（ＡＴＭ）回線であり、上記論理チャネル識別子は、ＶＰＩ及びＶＣＩであることを特徴とするパケット転送制御方法。
【請求項１９】それぞれ異なるバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）に属する複数のローカル・エリア・ネットワーク（ＬＡＮ）を収容するルータ装置におけるＶＰＮ識別情報の設定方法であって、
上記ルータ装置は、上記複数のＬＡＮの一部のＬＡＮからは第１のプロトコルでカプセル化されたパケットを受信し、上記複数のＬＡＮの他のＬＡＮからは第２のプロトコルでカプセル化されたパケットを受信し、そして、メモリを有し、上記方法は、
上記一部のＬＡＮから受信したパケットが何れのＶＰＮに属するのかを識別するための第１の識別子を上記メモリに設定し、
上記他のＬＡＮから受信したパケットが何れのＶＰＮに属するのかを識別するための第２の識別子を上記メモリに設定し、
上記第２の識別子は上記第１の識別子とは異なることを特徴とする。
【請求項２０】請求項１９に記載のＶＰＮ識別情報の設定方法であって、
上記第１の識別子と、ＶＰＮに割り当てられているＶＰＮ番号との対応関係を示す第１のテーブルを設定し、
上記第２の識別子と、ＶＰＮに割り当てられているＶＰＮ番号との対応関係を示す第２のテーブルを設定する、ステップを更に有することを特徴とするＶＰＮ識別情報の設定方法。
【請求項２１】請求項１９又は請求項２０の何れかに記載のＶＰＮ識別情報の設定方法であって、
上記第１のプロトコルは非同期転送モードプロトコルであり、上記第１の識別子はＶＰＩ及びＶＣＩであり、

5

上記第２のプロトコルはフレームリレーであり、上記第２の識別子はＤＬＣＩであることを特徴とするＶＰＮ識別情報の設定方法。

【請求項２２】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容するルータ装置におけるパケット転送制御方法であって、

レイヤ２に相当するプロトコルによるカプセルヘッダが付与されたＩＰパケットを受信し、

上記カプセルヘッダ内の情報を用いて、上記受信したＩＰパケットが何れのＶＰＮに属するかを決定する、ステップを有することを特徴とするパケット転送制御方法。

【請求項２３】複数のバーチャル・プライベート・ネットワーク（以下、「ＶＰＮ」という。）を収容するルータ装置であって、

レイヤ２に相当するプロトコルによるカプセルヘッダが付与されたＩＰパケットを受信するインタフェース部と、

上記カプセルヘッダ内の情報を用いて、上記受信したＩＰパケットが何れのＶＰＮに属するかを決定する手段、とを有することを特徴とするルータ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はルータ装置、そのパケット転送制御方法及びルータ装置内のルーティング情報設定方法に係り、特にインターネットにおける仮想専用網（ＶＰＮ：Virtual Private Network）を構築するルータ装置、その転送制御方法、その設定方法に関する。

【０００２】

【従来の技術】従来、異なる地域に存在する複数の企業内網をネットワークにより接続する場合、企業は企業内網を専用線で相互接続することによって、外部のネットワークから隔絶した（つまりセキュリティが確保された）ネットワークを構築していた。しかし、専用線を使用するとネットワークコストが上昇してしまうという問題があった。このため、廉価で使用できるインターネットの普及に伴い、インターネットを利用して低コストの仮想的な専用線網（以下、ＶＰＮ：Virtual Private Networkと呼ぶ）を構築する技術に対する要求が高まってきた。この技術は、ＩＰ（Internet Protocol）ネットワークが提供するＩＰあるいはＩＰの下位レイヤの機能を用いて、専用網を仮想的にインターネット上に構築するものである。この技術により、ＩＰネットワーク上でも、外部のネットワークから隔絶された安全でかつ何らかの品質保証が行えるネットワークを構築することができる。

【０００３】ＶＰＮを実現する方式としては、ＶＰＮを提供するインターネットサービスプロバイダ（以下、ＩＳＰと呼ぶ）のネットワークの入り口でカプセル化を行い、ＩＳＰのネットワーク上ではこのカプセル化したヘッダに基づき転送を行い、ネットワークの出口でカプセルヘッダをはずす方式により転送を行う方式がある。インターネットの内部ではＶＰＮ固有のカプセル化ヘッダを用いることにより、セキュリティの確保されたＶＰＮを構成することが出来る。このカプセル化の具体的なプロトコルとしては、ＩＰカプセル化、ＭＰＯＡ（Multi Protocol OverATM）、ＭＰＬＳ（Multi Protocol Label Switching）等の方式があり、２０００年５月現在、IETFなどの標準化団体で標準化が進められている。

【０００４】

【発明が解決しようとする課題】ＩＰアドレスには、グローバルＩＰアドレスと、プライベートＩＰアドレスとがある。グローバルＩＰアドレスは世界的に一意に定められるものであるのに対し、プライベートＩＰアドレスは企業が自由に定めることができるものである。企業内網では、プライベートＩＰアドレスが用いられる場合が多い。したがって、企業がＶＰＮサービスを利用する場合においても、プライベートＩＰアドレスを使用できることが望ましい。この場合、複数のＶＰＮ間で同一のＩＰアドレスが使用される可能性がある。複数のＶＰＮ間のＩＰアドレスがバッティングする場合、それぞれのＶＰＮのパケットを正しく処理するため、ＩＳＰネットワークの入り口に位置し、かつ、ＶＰＮに属するＬＡＮ（Local Area Network）を収容するルータ（以下、ＶＰＮエッジルータと呼ぶ）は、ＶＰＮ毎のルーティングテーブルを保持する必要がある。ＶＰＮエッジルータは、パケットを受信すると、そのパケットがどのＶＰＮに属するＬＡＮからのパケットかを判定する。その後、ＶＰＮエッジルータは、当該ＶＰＮ用のルーティングテーブルを検索してＩＳＰ内ネットワークでの転送先の決定、およびカプセル化を行う。ＶＰＮエッジルータはＶＰＮ毎にルーティングテーブルを保持しているので、ＶＰＮエッジルータは、異なるＶＰＮから受信した同一の宛先ＩＰアドレスを持つパケットを混同せず、正しく転送することができる。

【０００５】前記ＶＰＮを識別する方式としては、例えば「日経コミュニケーション」、１９９９年１０月１８日号、ｐ．１００、に記載されているように、ユーザ回線インターフェース単位に、ＶＰＮを一意に識別するためのＶＰＮ－ＩＤを割り当て、このＶＰＮ－ＩＤによりＶＰＮ識別を行う方式がある。すなわち、ＶＰＮの識別単位は物理インターフェース毎ということになる。この場合、物理インターフェース一つがＶＰＮ一つに対応している必要がある。

【０００６】しかし前記の方式では、企業ネットワークからＩＳＰネットワークまでが、一つの物理回線で接続されている必要がある。また、一つの企業ネットワークを複数のＶＰＮと接続させたい場合、そのＶＰＮの数だけ物理回線を用意する必要がある。さらに、ＶＰＮエッジルータは、収容するＶＰＮの数だけ物理インターフェ

ースを保持する必要がある。このため、ＶＰＮエッジルータが収容するＶＰＮの数が大きくなると、ＶＰＮエッジルータの物理インターフェース数及びルータ自体の数も大きくなるという問題がある。

【０００７】企業ネットワークからＶＰＮサービスを行うＩＳＰネットワークまでのアクセス手段として、別のＩＳＰあるいはキャリアが提供するＡＴＭ網やフレーム・リレー等を用いる場合、ＩＳＰの入り口では１つの物理インターフェース内に複数の論理的なチャネルが多重されているため、物理インターフェースでＶＰＮ識別を行うことはできないという問題もある。

【０００８】本発明の目的は、物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮ識別を可能にすることである。

【０００９】また、本発明の他の目的は、ルータがＬＡＮを収容する際、ＩＰの下位レイヤとして複数の異なるプロトコルを用いる場合でも、それぞれのプロトコルに対応した適切なＶＰＮ識別情報を用いてＶＰＮ識別を行うことを可能にすることである。

【００１０】

【課題を解決するための手段】前記課題を解決するため、本発明のＶＰＮエッジルータは、物理インターフェースに多重化されている論理的なチャネルを識別するためのチャネル番号を用いてＶＰＮを識別する。論理的なチャネル番号として、ＩＰの下位レイヤの情報、例えば、ＯＳＩモデルで規定されているレイヤ２に相当する情報を用いる。論理的なチャネル番号の例をいくつか挙げると、ＩＰパケットの下位レイヤがＡＴＭの場合は、ＶＰＩ、ＶＣＩ等のヘッダ情報を、下位レイヤがフレームリレーの場合はＤＬＣＩを論理的なチャネル番号として用いることができる。また、ＩＰパケットがＬ２ＴＰ（Layer2 Tunneling Protocol）で規定されているＬ２ＴＰヘッダでカプセル化されている場合には、Ｌ２ＴＰカプセルヘッダ内の情報（トンネルID、セッションID等）を論理的なチャネル番号として用いることができる。下位レイヤがイーサーネットで、IEEE802.1Qで規定されるＶＬＡＮ　Ｔａｇを用いてＶＰＮの識別が行われる場合、前記論理的なチャネル番号としてＶＬＡＮＴａｇを用いることができる。IPパケットがPPP Over Ethernetカプセル化方式で規定されているカプセル情報でカプセル化されている場合には、PPP Over Ethernetカプセル化方式で規定されているカプセル情報（セッションID等）を論理的なチャネル番号として用いることができる。

【００１１】さらに、ＶＰＮエッジルータに、ＶＰＮ識別に用いる識別子を設定するためのＶＰＮ識別子設定テーブルを設ける。この設定をＶＰＮエッジルータを管理するＩＳＰの管理者が行えるようにするため、ＶＰＮエッジルータにユーザインターフェースを設ける。ＩＰの下位レイヤがＡＴＭの場合を例に説明すると、ＶＰＮ識別を物理インターフェースで行う場合には、前記ＶＰＮ識別子設定テーブルに物理インターフェースと設定する。また、ＶＰＮ識別をＶＰＩ、ＶＣＩで行う場合には、前記ＶＰＮ識別子設定テーブルにＶＰＩ、ＶＣＩと設定する。

【００１２】ＶＰＮ識別子設定テーブルの設定単位は、物理インターフェース毎としてしてもよいし、下位レイヤとして同一のプロトコルが使用される複数の回線を収容するインターフェースカード単位でもよい。また、１つの物理インターフェース内に下位レイヤとして複数のプロトコルが多重化されている場合（例えばフレームリレーとＰＰＰが時分割多重されている回線）は、その設定単位は、物理インターフェースとＩＰの下位レイヤのプロトコルとの組合わせでもよい。

【００１３】ＩＳＰがＶＰＮを収容する際、ＩＰの下位レイヤにＡＴＭを用い、ＶＰＮ識別子としてＶＰＩ、ＶＣＩを用いる場合を例にＶＰＮエッジルータの動作を具体的に説明する。ＶＰＮエッジルータはパケットを受信すると、まず、ＶＰＮ識別子設定テーブルの設定に従い、ＶＰＮ識別子（本例の場合、ＶＰＩ、ＶＣＩと設定されている）および検索すべきＶＰＮ識別テーブルを決定する。本例の場合、ＶＰＮエッジルータは、ＶＰＩ、ＶＣＩとＶＰＮとの対応が示されているテーブルを検索することになる。ＶＰＮエッジルータは、ＶＰＩ、ＶＣＩを検索キーにしてＶＰＮ識別テーブルの検索を行い、受信したパケットがどのＶＰＮに属しているかを判定する。その判定が終了すると、ＶＰＮエッジルータは、受信したパケットが属するＶＰＮ用のルーティングテーブルを検索し、ＩＳＰネットワーク内の次の転送先を決定し、ネットワーク内でＶＰＮ識別のために使用されるカプセル化ヘッダ情報の生成を行う。ＶＰＮエッジルータは、パケットにヘッダ情報を付与し、決定した次の転送先へパケットを送出する。

【００１４】以上の説明のように、本発明では、物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮ識別を行うため、ＶＰＮエッジルータにＶＰＮ毎に物理インターフェースを用意する必要がない。また、一つの企業ネットワークを複数のＶＰＮと接続させたい場合、そのＶＰＮの数だけ論理的なチャネルを用意すればよく、ＶＰＮの数だけ物理的な回線を用意する必要が無い。また、企業ネットワークからＶＰＮサービスを行うＩＳＰネットワークまでのアクセス手段として、別のＩＳＰあるいはキャリアが提供するＡＴＭ網やフレーム・リレー等を用いる場合においても、論理的なチャネルでＶＰＮ識別が行われるため、ＶＰＮを実現することができる。

【００１５】さらに、本発明によれば、ＩＳＰの管理者は、ＩＰの下位レイヤのプロトコル毎にＶＰＮ識別子を選択し、そのＶＰＮ識別子をＶＰＮ識別子設定テーブルに設定することができるため、ＶＰＮを収容する際、下

位レイヤに様々のプロトコルを用いることができる。

【００１６】

【発明の実施の形態】図１は、本発明のＶＰＮエッジルータを用いて構成したＶＰＮの一実施例を説明するための図である。以下では、下位レイヤとは、ＩＰパケットをカプセル化するプロトコルを意味するものとする。また、ＩＰパケットをＩＰヘッダでカプセル化する場合にも、便宜上、このカプセルヘッダを下位レイヤのヘッダとして表記することとする。

【００１７】ＩＳＰネットワーク（５）は、ネットワークのバウンダリに位置するエッジルータ（９、１０）と、ネットワークコアに位置するコアルータ（１７）とを有する。図１では、コアルータ（１７）は一つしか示されていないが、その数はこれに限定されるものではない。ＩＳＰネットワーク（５）内部ではＭＰＬＳ（ＡＴＭによる）によりカプセル化が行われＶＰＮが実現されるものとする。上述のように、カプセル化の仕方はこれに限られない。ＩＳＰネットワーク（５）は、エッジルータ（９）を介してＬＡＮ１（１）とＬＡＮ２（２）を収容し、エッジルータ（１０）を介してＬＡＮ３（３）とＬＡＮ４（４）を収容する。ＬＡＮ１（１）とＬＡＮ３（３）は同一企業ＡのＬＡＮであり、これらのＬＡＮ間でＶＰＮを構成する。また、ＬＡＮ２（２）とＬＡＮ４（４）は同一企業ＢのＬＡＮであり、これらのＬＡＮ間でもＶＰＮを構成する。企業Ａ、企業ＢのＶＰＮをそれぞれＶＰＮＡ（７）、ＶＰＮＢ（８）と呼ぶことにする。

【００１８】ＬＡＮ１とＬＡＮ２は、ＩＳＰネットワーク（５）とは別のＩＳＰまたはキャリアが提供するＡＴＭ網（６）を介し、回線（１１）に論理的に多重化されてエッジルータ（９）に接続されている。回線（１１）とエッジルータ（９）の物理インターフェースを（１２）とする。物理インタフェースとは、ルータと回線との接続点という意味である。一方、ＬＡＮ３（３）とＬＡＮ４（４）はそれぞれＲＦＣ２６１５で規定されているＰＯＳ（PPP Over SONET）を用い、回線（１３）、（１４）を介してエッジルータ（１０）に接続されている。回線（１３）、（１４）とエッジルータの物理インターフェースをそれぞれ（１５）、（１６）とする。

【００１９】本実施例では、ＬＡＮ１とＬＡＮ２が属しているＶＰＮを識別する識別子としてＶＰＩ、ＶＣＩが用いられる。エッジルータ（９）内に設けられたＶＰＮ識別子設定テーブルにおいて、物理インターフェース（１２）に対応するエントリには、ＶＰＩ、ＶＣＩと設定される。エッジルータ（１０）は、ＬＡＮ３とＬＡＮ４が属しているＶＰＮを識別する識別子として物理インターフェースに与えられている番号を用いる。エッジルータ（１０）内に設けられたＶＰＮ識別子設定テーブルにおいて、物理インターフェース（１５）、（１６）に対応するエントリには、物理インターフェースと設定される。ＶＰＮ識別子設定テーブルは後述される。

【００２０】また、エッジルータ（９）内には、ＶＰＮ識別子と、当該ＶＰＮ識別子を有するパケットが何れのＶＰＮに属するかを示す情報（以下、ＶＰＮ番号という。）との対応関係を示すＶＰＮ識別テーブルが設けられている。上記ＶＰＮＡ、ＶＰＮＢがＶＰＮ番号に該当する。さらに、エッジルータ（９）内には、宛先ＩＰアドレスと、出力方路及び出力パケットのカプセルヘッダ情報との関係を示すルーティングテーブルが設けられている。このルーティングテーブルはＶＰＮＡ用のものと、ＶＰＮＢ用のものとが用意される。ＶＰＮ識別テーブル及びルーティングテーブルについても後述される。

【００２１】エッジルータ（９）は、ＬＡＮ１から送信されたＬＡＮ３宛のＩＰパケットを受信すると、ＶＰＮ識別子設定テーブルの設定に従い、ＶＰＮ識別子としてＶＰＩ、ＶＣＩを用いることを決定する。ＶＰＮ識別子を決定した後、エッジルータ（９）は、ＶＰＩ、ＶＣＩとＶＰＮとの対応が示されているＶＰＮ識別テーブルを検索し、当該パケットがＶＰＮＡに属するパケットであると判定する。次に、エッジルータ（９）は、宛先ＩＰアドレスを検索キーとしてＶＰＮＡ用のルーティングテーブルを検索し、次転送先のコアルータ（１７）を決定し、そして、コアルータ行きのＶＰＮＡに属するパケットのカプセルヘッダを決定する。このカプセルヘッダが付与されたパケットは、コアルータ（１７）へ転送される。

【００２２】コアルータ（１７）は、カプセルヘッダ、すなわち、ＶＰＩ、ＶＣＩと、次転送先との対応関係を示すルーティングテーブルを有しており、受信パケットのカプセルヘッダを検索キーにして次転送先（エッジルータ（１０））、および次のカプセルヘッダを決定し、前記カプセルヘッダを付与してエッジルータ（１０）へ送信する。

【００２３】エッジルータ（１０）は、エッジルータ（９）と同様の構成であり、エッジルータ（９）と同様にして、受信パケットのカプセルヘッダを検索キーにしてＶＰＮ識別を行い、ＶＰＮＡに属するパケットであることを判定する。次に宛先ＩＰアドレスを検索キーとしてＶＰＮＡ用のルーティングテーブルを検索して転送先を決定し、カプセルヘッダをはずしてＬＡＮ３へパケットを転送する。

【００２４】エッジルータ（９）は、物理インターフェースに多重された論理的なチャネル番号によりＶＰＮを識別し、当該ＶＰＮのルーティングテーブルを検索するので、一つの回線に論理的に多重されたＶＰＮを識別することが可能となる。また、これにより、企業Ａが用いるＩＰアドレスとと企業Ｂが用いるＩＰアドレスとがバッティングする場合でも、正しいあて先への転送が可能となる。

【００２５】ＶＰＮＢ内のＬＡＮ４からＬＡＮ２へパケ

ットを送信する場合も上記の場合と同様の手続により送信が行われるが、ＬＡＮ４から送信されたＬＡＮ２宛のＩＰパケットを受信したエッジルータ（１０）は、ＶＰＮ識別子として物理インターフェースを用いる点が上記の場合と異なる。

【００２６】図２は、図１に示される実施例の変形例を説明するための図である。本実施例では、ＬＡＮ１とＬＡＮ２は、別回線（１８）、（１９）を介して、直接、ＩＳＰネットワーク（５）内の多重化装置（２０）に収容される。多重化装置（２０）において、ＶＰＮＡ、ＶＰＮＢごとに異なるＶＰＩ、ＶＣＩが割り当てられる。エッジルータ（９）は、図１の場合と同様に、ＶＰＩ、ＶＣＩを用いてＶＰＮ識別を行う。

【００２７】図３は、図１に示される実施例の他の変形例を説明するための図である。

【００２８】図３では、図１に示したネットワーク構成に、ＬＡＮ５（２１）が付け加えられており、ＬＡＮ２、ＬＡＮ４及びＬＡＮ５の間でＶＰＮＢが構成されている。ＬＡＮ５（２１）はＰＯＳを用い、回線（２２）でエッジルータ（９）に接続されている。回線（２２）とエッジルータの物理インターフェースを（２３）とする。

【００２９】エッジルータ（９）は、図１の説明と同様に、ＬＡＮ１とＬＡＮ２が属しているＶＰＮを識別する識別子としてＶＰＩ、ＶＣＩを用いる。一方、エッジルータ（９）は、ＬＡＮ５が属しているＶＰＮを識別する識別子として物理インターフェースを用いる。エッジルータ（９）内のＶＰＮ識別子設定テーブルには、物理インターフェース（２３）に対応するエントリに物理インターフェースと設定される。本実施例では、エッジルータ（９）内に、ＶＰＩ、ＶＣＩとＶＰＮとの対応が示されているＶＰＮ識別テーブルと、物理インターフェースとＶＰＮとの対応が示されているＶＰＮ識別テーブルとの２種類のＶＰＮ識別テーブルが設けられている。その詳細は後述される。

【００３０】例えば、ＬＡＮ５から送信されたＬＡＮ４宛のＩＰパケットを受信した場合、エッジルータ（９）は、ＶＰＮ識別子設定テーブルの設定に従い、ＶＰＮ識別子として物理インターフェースの番号を用いることを決定する。ＶＰＮ識別子を決定した後、エッジルータ（９）は、物理インターフェースの番号を検索キーとして、物理インターフェースとＶＰＮとの対応が示されているＶＰＮ識別テーブルを検索し、そのＩＰパケットがＶＰＮＢに属するパケットであることを判定する。次に、宛先ＩＰアドレスを検索キーとしてＶＰＮＢ用のルーティングテーブルを検索し、次転送先のコアルータ（１７）を決定し、その決定したコアルータに送信されるパケットのカプセルヘッダを決定する。このカプセルヘッダをパケットに付与し、コアルータ（１７）に転送する。

【００３１】本実施例では、異なる下位プロトコル毎にＶＰＮ識別子を定め、各ＶＰＮ識別子対応にＶＰＮ識別テーブルを設けている。このようにすることにより、一つのルータで異なる下位プロトコルに対応する際の自由度が増す。すなわち、本実施例によれば、エッジルータに収容しようとする下位プロトコルに応じて、ＶＰＮ識別子設定テーブル内のＶＰＮ識別子を設定し、そのＶＰＮ識別子に対応するＶＰＮ識別テーブルを設定しさえすれば、エッジルータにおいて様々な下位プロトコルを収容することが可能となる。

【００３２】次に、本発明のＶＰＮエッジルータの詳細を説明する。ＶＰＮを構成する上で、ネットワークの構成は図１～図３に示したもの以外にも、多様な構成が考えられる。そこで、図１～図３のネットワークを構成する場合のＶＰＮエッジルータの構成に限定して説明するのではなく、より一般的に、本発明ＶＰＮエッジルータの構成を説明する。

【００３３】図４から図８を用いて、ＶＰＮエッジルータ（９）の一構成例を説明する。ＶＰＮエッジルータ（１０）の構成もこれと同様である。

【００３４】図４は、本発明のＶＰＮエッジルータ（９）の一構成例を示す図である。制御部（５０）は、下位レイヤ処理部（５３、５４）、パケットレイヤ処理部（５２）及びスイッチ（５１）と接続されており、ＶＰＮエッジルータ全体の制御及びルーティング処理などを行う。下位レイヤ処理部（５３、５４）は、回線（５５、５６）を収容するとともに、ＩＰの下位レイヤの終端を行う。パケットレイヤ処理部（５２）は、下位レイヤ処理部（５３、５４）から下位レイヤの情報及びＩＰパケットを受け取り、その下位レイヤの情報とそのＩＰパケットのヘッダ情報とを用いてパケットの転送先を決定する。スイッチ（５１）は複数の入出力ポートを有しており、それらのポートは、パケットレイヤ処理部と接続されている。スイッチ（５１）は、例えば、クロスバスイッチで構成される。スイッチ（５１）は、パケットレイヤ処理部（５２）からパケットを受信すると、パケットレイヤ処理部（５２）において決定されたパケットの転送先に対応する出力ポートに、そのパケットを出力する。前記制御部（５０）には制御端末（５７）が接続される。前記制御端末により、ルータの管理者は、ルータ内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル及びルーティングテーブルの設定等を行うことが可能である。受信回線５５－１、５５－２、５５－３及び５５－４とルータ（９）との接続点には、それぞれ、物理インタフェース番号１、２、３及び４が割り当てられている。

【００３５】図５は、パケットレイヤ処理部（５２）の一構成例を示す図である。下位レイヤ処理部ＩＦ（１００、１０６）、スイッチＩＦ（１０３、１０４）及び制御部ＩＦ（１１０）は、それぞれ、下位レイヤ処理部

（５３、５４）とのインタフェース、スイッチ（５１）とのインタフェース及び制御部（５０）とのインタフェースである。本実施例の特徴の一つは、ＶＰＮ識別子設定テーブル（１５０）、ＶＰＮ識別テーブル（１５１）及びＶＰＮ用のルーティングテーブル（１５２）を設けた点にある。これらはメモリ上に構成される。これらは、それぞれ、物理的に異なるメモリ上に構成されてもよいし、同一のメモリ上の異なる領域に構成されてもよい。この構成の仕方の差異は本発明を実施する上で本質的なものではない。ＶＰＮ識別子設定テーブル（１５０）、ＶＰＮ識別テーブル（１５１）、ルーティングテーブル（１５２）及びここで説明しなかったその他のブロックの機能・構成は、以下で説明するルータ（９）のパケット処理動作と併せて説明する。

【００３６】下位レイヤ処理部（５３）が収容している回線（５５）からパケットを受信し、下位レイヤ処理部（５４）が収容している回線（５６）へパケットを転送する場合を例に引き、ルータ（９）のパケット処理を説明する。

【００３７】下位レイヤ処理部（５３）は、ＬＡＮからパケットを受信すると、ＩＰの下位レイヤのプロトコルを終端する。下位レイヤ処理部（５３）は、ＩＰパケットとともに、パケットを受信した物理インターフェース番号（以下、受信物理インターフェース番号と呼ぶ）、下位レイヤのプロトコル種別、ＶＰＮ識別子として用いる下位レイヤのカプセルヘッダ情報等をパケットレイヤ処理部（５２）へ転送する。

【００３８】パケットレイヤ処理部（５２）内の下位レイヤ処理部インターフェース（１００）は、下位レイヤ処理部（５３）から転送されたＩＰパケット、受信物理インターフェース番号、下位レイヤのプロトコル種別及びＶＰＮ識別子として用いる下位レイヤのカプセルヘッダ情報をパケット転送処理部（１０１）へ転送する。パケット転送処理部（１０１）は、受信したＩＰパケットからＩＰヘッダ情報を抽出し、このＩＰヘッダ情報、受信物理インターフェース番号、下位レイヤのプロトコル種別及びＶＰＮ識別子として用いる下位レイヤのカプセルヘッダ情報をＶＰＮ識別・ルーティングテーブル検索処理部（１０２）へ転送する。ＩＰパケット本体はパケット転送処理部（１０１）内に一時的に蓄積される。

【００３９】ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、まず受信物理インターフェース番号、下位レイヤのプロトコル種別等を検索キーとしてＶＰＮ識別子設定テーブル（１５０）を検索し、ＶＰＮ識別子を決定する。

【００４０】図６は、ＶＰＮ識別子設定テーブル（１５０）の一構成例を示す。各エントリは、物理インターフェース番号（２００）、下位レイヤプロトコル（２０３）及びＶＰＮ識別子（２０１）とを有する。下位レイヤプロトコルがＡＴＭのエントリには、パケットの転送優先度を示すＣＬＰのフィールドを設けてあるが、このフィールドはなくてもよい。上述の通り、エッジルータ（９）の管理者は、制御端末（５７）から、ＶＰＮ識別子を設定することができる。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、検索キーとして受信物理インターフェース番号を用いて検索を行い、ＶＰＮ識別子（２０１）を決定する。例えば、受信物理インタフェース番号が１の場合、ＶＰＮ識別子はＶＰＩ、ＶＣＩとなり、受信物理インタフェース番号が３の場合、ＶＰＮ識別子は物理インタフェース番号となる。本実施例のように、ＣＬＰフィールドを設ける場合には、ＶＰＮ識別子として、ＶＰＩ、ＶＣＩとＣＬＰとの組み合わせ、物理インタフェース番号とＣＬＰとの組み合わせを用いてもよい。ＶＰＮ識別子にＣＬＰ（２０４）を含めた場合のメリットについては後述する。一つの物理インタフェースに対して、複数のＶＰＮに属するパケットが論理的に多重されて送信される場合、受信物理インタフェース番号からは、そのパケットがどのＶＰＮに属するのか判別することができない。しかし、その下位レイヤがＡＴＭの場合、ＶＰＩ、ＶＣＩをＶＰＮ識別子に用いれば、そのパケットがどのＶＰＮに属するのかを識別することが可能となる。一つの物理インタフェースに対して、一つのＶＰＮに属するパケットしか送信されない場合には、物理インタフェース番号でＶＰＮを識別することが可能である。検索キーとして、下位レイヤのプロトコル（２０３）と物理インターフェース番号（２０１）との組み合わせを用いてもよい。例えば、物理インターフェース番号４に接続される回線が時分割多重回線であり、前記回線に、下位レイヤのプロトコルとしてフレームリレーを用いたパケットと、ＰＰＰ(Point to Point Protocol)プロトコルを用いたパケットが多重されているとする。また、下位レイヤプロトコルがフレームリレーのエントリに対しては、ＶＰＮ識別キーとしてＤＬＣＩが設定されており、下位レイヤプロトコルがＰＰＰのエントリに対しては、ＶＰＮ識別キーとしてタイムスロット番号が設定されているとする。この場合、受信物理インタフェース番号４のみを検索キーとして検索しても、ＶＰＮ識別子がＤＬＣＩであるかタイムスロット番号であるかが一意に定まらない。そこで、この場合には、受信物理インタフェース番号と下位レイヤプロトコルとの組み合わせにより、ＶＰＮ識別子を検索する。

【００４１】ＶＰＮ識別子が決定されると、ＶＰＮ識別・ルーティングテーブル検索処理部は、そのＶＰＮ識別子を検索キーとしてＶＰＮ識別テーブル（１５１）を検索し、受信パケットが属しているＶＰＮを決定する。

【００４２】図７（ａ）、（ｂ）は、ＶＰＮ識別テーブル（１５１）の一構成例を示す。どちらのＶＰＮ識別テーブルにおいても、各エントリは、ＶＰＮ識別子（２０１）とＶＰＮ番号（２５０）とを有する。

【００４３】図７（ａ）は、ＶＰＮ識別子（２０１）と

してＶＰＩ、ＶＣＩを用いるテーブルの例を示している。図７（ａ）のＣＬＰフィールド（２０４）及び装置内優先度情報フィールド（２５１）は設けなくても良い。装置内優先度情報フィールド（２５１）とは、装置内におけるパケット処理の優先度情報を示すフィールドである。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、検索キーとして前記のＶＰＮ識別子設定テーブルの検索により決定したＶＰＮ識別子に従い、検索キーとしてパケットヘッダ内のＶＰＮ識別情報を用いて検索を行い、ＶＰＮ番号（２５０）を決定する。本実施例のように、ＶＰＮ識別テーブル（１５１）にＣＬＰフィールド（２０４）及び装置内優先度情報フィールド（２５１）を設ける場合には、検索キーとしては、パケットの転送優先度を示すＣＬＰ（２０４）とＶＰＩ、ＶＣＩの組み合わせを用いてもよい。ＣＬＰを検索キーに含めることにより、同一のＶＰＮ番号に属するパケットに対して、異なる装置内優先度情報を定めることができる。例えば、”ＶＰＩ、ＶＣＩ＝ａ”かつ”ＣＬＰ＝０”の場合は、”装置内優先度＝ａ”、”ＶＰＩ、ＶＣＩ＝ａ”かつ”ＣＬＰ＝１”の場合は、”装置内優先度＝ｂ”のように、同一のＶＰＮ番号に属するパケットに対して異なる装置内優先度情報を定めることができる。

【００４４】図７（ｂ）は、ＶＰＮ識別子（２０１）として物理インターフェース番号（２５２）を用いるテーブルの例を示している。パケット処理の優先制御を行わないのであれば、図７（ｂ）の装置内優先度情報フィールド（２５１）は設けなくても良い。

【００４５】上記以外のＶＰＮ識別子、例えば、ＤＬＣＩ、タイムスロット番号等が使用される場合には、図７（ａ）、（ｂ）と同様のテーブルを構成すればよい。すなわち、ＶＰＮ識別テーブル（１５１）は、ＶＰＮ識別子毎に設けられ、これらの設定は、制御端末（５４）から設定される。ＶＰＮ識別子毎に設けられたＶＰＮ識別テーブル（１５１）は、同一のメモリ上に構成されても良いし、それぞれ、異なるメモリ上に構成されてもよい。

【００４６】ＶＰＮ番号が決定されると、ＶＰＮ識別・ルーティングテーブル検索処理部は、そのＶＰＮ番号に対応するＶＰＮ用のルーティングテーブル（１５２）を検索し、出力方路及びそのＶＰＮ番号に属するパケットに付加されるＶＰＮ用の出力カプセルヘッダ情報を決定する。

【００４７】図８は、ＶＰＮ用ルーティングテーブル（１５２）の一構成例を示す。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、収容するＶＰＮ毎にこのＶＰＮ用ルーティングテーブル（１５２）を保持する。このＶＰＮ毎に設けられたＶＰＮ用ルーティングテーブル（１５２）は、同一のメモリ上に構成されても良いし、それぞれ異なるメモリ上に構成されてもよい。ＶＰＮ用ルーティングテーブル（１５２）は宛先ＩＰアドレス（３００）と出力方路番号（３０１）と出力カプセルヘッダ情報（３０２）とを有する。出力方路番号（３０１）は、スイッチ等でパケットを所望のインターフェースに転送するための装置内識別子である。出力カプセルヘッダ情報（３０２）は、ＩＳＰネットワーク（５）内で用いるカプセルヘッダ情報である。ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、検索キーとしてＩＰヘッダ内の宛先ＩＰアドレスを用いて、前記のＶＰＮ識別テーブルの検索により決定したＶＰＮ番号（２５０）に対応するＶＰＮ用のルーティングテーブルの検索を行い、出力方路番号（３０１）及び出力カプセルヘッダ情報（３０２）を決定する。本実施例では、ＶＰＮ毎にＶＰＮ用ルーティングテーブル（１５２）を設けているので、複数のＶＰＮにおいて同一のＩＰアドレスが使用されていても、正しい出力方路を決定することができる。



【００４８】出力方路番号（３０１）と出力カプセルヘッダ情報（３０２）とが決定されると、ＶＰＮ識別・ルーティングテーブル検索処理部（１０２）は、その決定した出力方路（３０１）と出力カプセルヘッダ情報（３０２）とをパケット転送処理部（１０１）に転送する。

【００４９】パケット転送処理部（１０１）は、スイッチＩＦ（１０３）を介して、蓄積していたＩＰパケット本体、出力方路番号（３０１）及び出力カプセルヘッダ情報（３０２）とをスイッチ（５１）に転送する。スイッチ（５１）は、パケット転送処理部（１０１）から受信したＩＰパケット本体と、その出力カプセルヘッダ情報（３０２）とを、その出力方路番号に対応する出力ポートに出力する。

【００５０】上記出力ポートに接続されているパケットレイヤ処理部（５２）、すなわち、パケットレイヤ処理部（５２）から送信されたＩＰパケット本体及びその出力カプセルヘッダ情報（３０２）を受信する側のパケットレイヤ処理部（５２）は、スイッチＩＦ（１０４）を介して、それらを受信する。ＩＰパケット本体及びその出力カプセルヘッダ情報（３０２）とを受信すると、パケット転送処理部（１０５）はこれらを下位レイヤ処理部ＩＦ（１０６）を介して下位レイヤ処理部（５４）に転送する。ＩＰパケット本体及びその出力カプセルヘッダ情報（３０２）とを受信すると、下位レイヤ処理部（５４）は、その出力カプセルヘッダ情報に基づきカプセルヘッダを生成し、そのカプセルヘッダによりＩＰパケット本体をカプセル化し、そして、そのカプセル化したパケットをコアルータ（１７）に送信する。

【００５１】以上、図４から図８を用いてＶＰＮエッジルータ装置の一構成例を説明した。本実施例のルータ装置を用いることにより、同一の物理インタフェースに、異なるＶＰＮに属するパケットが送信される場合であっても、それらが属するＶＰＮを識別することが可能となる。また、同一のエッジルータが、異なるＩＰの下位プ

ロトコルを用いる複数のＬＡＮを収容する場合でも、それぞれの下位プロトコルに対応した適切なＶＰＮ識別子をＶＰＮ識別子設定テーブルに設定することができるので、ＶＰＮ構築の自由度が増す。

【００５２】本実施例では、ＶＰＮ用ルーティングテーブルの検索結果として出力カプセルヘッダ情報を直接出力しているが、出力カプセル番号を出力するようにしてもよい。この出力カプセル番号は、出力側の下位レイヤ処理部においてカプセルヘッダを付与するための装置内識別子である。この場合、出力側の下位レイヤ処理部にカプセル番号とカプセルヘッダとをペアにしたヘッダ生成テーブルを設ける。出力側の下位レイヤ処理部は、検索キーとそてカプセル番号を用いてヘッダ生成テーブルを検索し、カプセルヘッダを決定する。

【００５３】本実施例で示したテーブルは論理的なテーブルであり、テーブル検索方法として、ツリー構造に代表される検索アルゴリズムを用いてもよいし、ＣＡＭ（Content Addressable Memory）を使った構成や、テーブルを逐次検索していく方式を採用してもよい。

【００５４】ＶＰＮエッジルータ装置が時分割多重回線を収容する場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、タイムスロット番号を加えてもよい。この場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにタイムスロット番号を設定してもよい。また、ＶＰＮ識別テーブルの検索キーとして、タイムスロット番号を用いてもよい。

【００５５】ＶＰＮエッジルータ装置がイーサネットを収容し、イーサネット上のパケットがIEEE802.1Qに従ってＶＬＡＮカプセル化されている場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、ＶＬＡＮ　Ｔａｇ情報を加えてもよい。この場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにＶＬＡＮ　Ｔａｇ情報を設定してもよい。また、ＶＰＮ識別テーブルの検索キーとして、ＶＬＡＮ　Ｔａｇ情報を用いてもよい。

【００５６】ＩＰパケットがＬ２ＴＰ（Layer2 Tunneling Protocol）で規定されているＬ２ＴＰヘッダでカプセル化されている場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにL2TPカプセルヘッダ内の各情報（トンネルID、セッションID等）を設定してもよい。

【００５７】また、IPパケットがPPP Over Ethernetカプセル化方式で規定されているカプセル情報でカプセル化されている場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、PPP Over Ethernetカプセル化方式で規定されているカプセル情報を加えてもよい。この場合、ＶＰＮ識別子として、ＶＰＮ識別子設定テーブルにPPP Over Ethernetカプセル化方式で規定されているカプセル情報（セッションID等）を設定してもよい。

【００５８】図９は、本発明のＶＰＮエッジルータ装置（９）の他の構成例を示す。インターフェースカード（４００、４０１）は、それぞれ、同一の下位レイヤのプロトコルを用いる回線を収容するカードである。例えばインターフェースカード（４００）はＡＴＭ用のインターフェースカードであり、ＡＴＭ回線（４０２）を収容する。また、インターフェースカード（４０１）はＰＯＳ用のインターフェースカードであり、ＰＯＳ回線（４０３）を収容する。インターフェースカード（４００、４０１）は着脱可能であり、ルータの管理者は、必要な下位レイヤプロトコル用のインターフェースカードを必要な数量だけ搭載することができる。各インターフェースカードには、各下位レイヤプロトコルに特有の処理を行う下位レイヤ処理部（４０５、４０６）が搭載されている。下位レイヤ処理部（４０５、４０６）の動作は、図４の下位レイヤ処理部（５３、５４）と同様である。パケット処理カード（４０７）は前記インターフェースカードからＩＰパケット等の情報を受け取り、パケットレイヤ処理を行うカードである。各パケット処理カード（４０７）は着脱可能であり、ルータの管理者は、必要な数量だけ搭載することができる。各パケット処理カード（４０７）には、図４、図５を用いて説明したパケットレイヤ処理部（５２）が搭載されている。管理者は、収容するインタフェースカードの種別、ＬＡＮとインタフェースカードとの間のアクセス網の構成に応じて、制御端末（５７）から、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの構成をフレキシブルに設定することができる。本実施例のＶＰＮエッジルータ装置のパケット処理動作は、図４から図８を用いて説明した動作と同様である。

【００５９】図１０から図１２は、図９のパケット処理カード（４０７）に収容されるインタフェースカードと、パケット処理カードに保持されるＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルとの関係を示す図である。図１０から図１２は、エッジルータに収容されるＬＡＮと、エッジルータ（９）の構成要素のうちインターフェースカードとパケット処理カードのみを示す。また、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルは論理的なものである。図１０から図１２では、同一インターフェースカード内の全物理インターフェースに対し、同じＶＰＮ識別子が使用される場合を示している。このため、ＶＰＮ識別子設定テーブルの検索キーとして物理インターフェース番号を設定する必要がないので、図１０から図１２では、その検索キーとしての物理インターフェース番号は省略されている。同一インターフェースカード内で、異なるＶＰＮ識別子が使用される場合は、上述のようにＶＰＮ識別子設定テーブルの検索キーとして物理インターフェ

ースを用いればよい。

【００６０】図１０は、パケット処理カード（４０７）にＡＴＭ用インターフェースカード（４００）が収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。ＬＡＮ１（４５０）はＶＰＮＡに属し、ＬＡＮ２（４５１）はＶＰＮＢに属しているとする。ＬＡＮ１、ＬＡＮ２からのパケットは多重化装置（４５２）で多重され、回線（４５３）を介してＡＴＭ用インターフェースカード（４００）に収容される。多重される際、ＬＡＮ１、ＬＡＮ２からのパケットにはＶＰＩ、ＶＣＩとしてそれぞれａ、ｂという値が割り当てられているとする。本実施例では、ＶＰＮ識別にはＶＰＩ、ＶＣＩを用いる。パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル（４５５）にはＶＰＮ識別子としてＶＰＩ、ＶＣＩが設定される。ＶＰＮ識別テーブル（４５６）には検索キーとしてＶＰＩ、ＶＣＩが設定される。ＶＰＮ用ルーティングテーブルとしてはＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）が設けられる。例えば、ＬＡＮ１からパケットを受信すると、ＡＴＭ用インターフェースカード（４００）内の下位レイヤ処理部（４０５）は、ＡＴＭプロトコルを終端し、ＩＰパケット本体及びＶＰＩ、ＶＣＩ、物理インターフェース番号等をパケット処理カード（４０７）に転送する。パケット処理カード（４０７）内のＶＰＮ識別・ルーティングテーブル検索処理部は、ＶＰＮ識別子設定テーブル（４５５）を検索し、ＶＰＮ識別子としてＶＰＩ、ＶＣＩを用いることを決定する。次に、受信パケットのＶＰＩ、ＶＣＩの値、”ａ”、を用いてＶＰＮ識別テーブル（４５６）を検索し、受信パケットがＶＰＮＡに属することを判定する。次にＶＰＮＡ用のルーティングテーブル（４５７）を検索し、出力方路、および出力カプセルヘッダ情報を決定する。

【００６１】図１１は、パケット処理カード（４０７）にＰＯＳ用インターフェースカード（４０１）が収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。

【００６２】ＬＡＮ１（４５０）はＶＰＮＡに属し、ＬＡＮ２（４５１）はＶＰＮＢに属しているとする。ＬＡＮ１、ＬＡＮ２はそれぞれ回線（５００）、（５０１）を介してＰＯＳ用インターフェースカード（４０１）に収容される。回線（５００）及び回線（５０１）とＰＯＳ用インターフェースカード（４０１）との物理インターフェース番号をそれぞれ１、２とする。この場合、ＶＰＮ識別には物理インターフェースを用いるため、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル（４５５）にはＶＰＮ識別子として物理インターフェース番号が設定される。ＶＰＮ識別テーブル（４５６）には検索キーとして物理インターフェース番号を設定する。ＶＰＮ用ルーティングテーブルとして、ＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）が設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、ＶＰＮ識別子としてＶＰＩ、ＶＣＩではなく、物理インターフェースを用いる点が異なる。

【００６３】図１２は、図９に図示していないが、パケット処理カード（４０７）に時分割多重回線用のインターフェースカード（５５０）が収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。ＬＡＮ１（４５０）、ＬＡＮ２（４５１）、ＬＡＮ３（５５１）ＬＡＮ４（５５２）はそれぞれＶＰＮＡ、ＶＰＮＢ、ＶＰＮＣ、ＶＰＮＤに属しているとする。ＬＡＮ１、ＬＡＮ２の下位プロトコルはフレームリレーとし、ＬＡＮ３、ＬＡＮ４の下位プロトコルはＰＰＰ（Point to Point Protocol）とする。ＬＡＮ１とＬＡＮ２からのパケットにはＤＬＣＩとしてそれぞれ１０、２０が割り当てられ、それらのパケットは、フレームリレー多重化装置（５５３）において、回線（５５４）に多重化される。さらに、時分割多重化装置（５５５）において、回線（５５４）、（５５６）、（５５７）が回線（５５８）に多重される。この際、回線（５５４）、（５５６）、（５５７）のデータにはそれぞれ、タイムスロット番号１、２、３が割り当てられるとする。ＬＡＮ１、ＬＡＮ２に対するＶＰＮ識別子としてはＤＬＣＩが用いられ、ＬＡＮ３、ＬＡＮ４に対するＶＰＮ識別子としてはタイムスロット番号が用いられるとする。この場合、ＶＰＮ識別子設定テーブル（４５５）における、下位レイヤプロトコル（５５９）がフレームリレーであるエントリに対しては、ＶＰＮ識別子としてＤＬＣＩ（５６０）が設定される。また、下位レイヤがＰＰＰであるエントリに対してはＶＰＮ識別子としてタイムスロット番号（５６１）が設定される。ＶＰＮ識別テーブルとして、２つのテーブル、すなわち、ＤＬＣＩとＶＰＮ番号の対応を示すＶＰＮ識別テーブル（５６２）と、タイムスロット番号とＶＰＮ番号の対応を示すＶＰＮ識別テーブル（５６３）とが設けられる。また、ＶＰＮ用ルーティングテーブルとして、ＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）、ＶＰＮＣ用ルーティングテーブル（５６４）及びＶＰＮＤ用ルーティングテーブル（５６５）が設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、ＶＰＮ識別子設定テーブル検索時に、検索キーとして下位レイヤプロトコル（５５９）を用いる点が異なる。またＶＰＮ識別子設定テーブル検索の結果、ＶＰＮ識別子として、ＬＡＮ１、ＬＡＮ２から受信

したパケットに関してはＤＬＣＩが使用され、ＬＡＮ３、ＬＡＮ４から受信したパケットに関してはタイムスロット番号が使用される点が異なる。

【００６４】図９から図１２では、１つのパケット処理カードが１つのインターフェースカードを収容する例について説明したが、パケット処理カードが複数のインターフェースカードを収容する構成をとってもよい。その際、収容する複数のインターフェースカードが異なる下位プロトコル用のものであってもよい。

【００６５】図１３は、パケット処理カード（４０７）に異なる下位プロトコル用のインターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す。インターフェースカード（４００）、（４０１）はそれぞれＡＴＭ用、ＰＯＳ用とする。図１３は、同一インターフェースカード内の全物理インターフェースに対し、ＶＰＮ識別子が同じ場合を示している。本実施例で、パケット転送カードは複数のインターフェースカードを収容するため、各インターフェースカード（４００）、（４０１）にはそれぞれカード番号１、２が割り当てられるている。また、ＶＰＮ識別子設定テーブル（４５５）の検索キーとして、カード番号（６０２）が設定される。ＬＡＮ１（４５０）、ＬＡＮ２（４５１）、ＬＡＮ３（５５１）ＬＡＮ４（５５２）はそれぞれＶＰＮＡ、ＶＰＮＢ、ＶＰＮＣ、ＶＰＮＤに属しているとする。ＬＡＮ１、ＬＡＮ２からのパケットは多重化装置（４５２）で多重され、回線（４５３）を介してＡＴＭ用インターフェースカード（４００）に収容される。多重される際、ＬＡＮ１、ＬＡＮ２からのパケットにはＶＰＩ、ＶＣＩとしてそれぞれａ、ｂという値が割り当てられるものとする。この場合、ＶＰＮ識別にはＶＰＩ、ＶＣＩを用いればよい。ＶＰＮ識別子設定テーブル（４５５）における、カード番号１のエントリ（６０３）に対しては、ＶＰＮ識別子としてＶＰＩ、ＶＣＩが設定される。ＬＡＮ３、ＬＡＮ４はそれぞれ回線（５００）、（５０１）を介してＰＯＳ用インターフェースカード（４０１）に収容される。回線（５００）、（５０１）とＰＯＳ用インターフェースカード（４０１）との物理インターフェース番号をそれぞれ１、２とする。この場合、ＶＰＮ識別には物理インターフェースを用いればよい。ＶＰＮ識別子設定テーブル（４５５）における、カード番号２のエントリ（６０４）に対しては、ＶＰＮ識別子として物理インターフェースが設定される。ＶＰＮ識別テーブルとしては、ＶＰＩ、ＶＣＩとＶＰＮ番号の対応を示すテーブル（６００）と、物理インターフェース番号とＶＰＮ番号の対応を示すテーブル（６０１）とが設けられる。ＶＰＮ用ルーティングテーブルとしてはＶＰＮＡ用ルーティングテーブル（４５７）、ＶＰＮＢ用ルーティングテーブル（４５８）、ＶＰＮＣ用ルーティングテーブル（５６４）、ＶＰＮＤ用ルーティングテーブル（５６５）とが設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、ＶＰＮ識別子設定テーブル検索時に、検索キーとしてカード番号（６０２）を用いる点が異なる。ここでは、ＡＴＭとＰＯＳとを収容する場合を示したが、この組み合わせに限られるものではない。例えば、ＰＯＳ用インタフェースカードをＦＲ用インタフェースカードに換えることも可能である。この場合、ＬＡＮ３及びＬＡＮ４からのパケットは、ＬＡＮ１及びＬＡＮ２と同様に、一本の回線に多重してＦＲ用インタフェースカードに入力されるように、ＤＬＣＩでＶＰＮを識別するようにしてもよい。

【００６６】以上、図９から図１３を用いて説明したように、本実施例のルータ装置によれば、管理者は、収容するインタフェースカードの種別に応じて、制御端末（５７）から、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの構成をフレキシブルに設定することができる。また、物理インターフェースに多重された論理的なチャネル番号によりＶＰＮを識別するので、一つの回線に論理的に多重されたＶＰＮを識別することが可能となる。

【００６７】図１４に、インタフェースカードを装着する際の、パケット処理カード（４０７）の設定手順の一例を示す。ＶＰＮエッジルータ（９）にインタフェースカードが装着された後、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル（４５５）が設定される（７０１、７０２）。ＶＰＮ識別子設定テーブルの設定は、装着するインタフェースカードの種別により、管理者が自由に設定することができる。次に、設定されたＶＰＮ識別子毎に、ＶＰＮ識別テーブルが設定される（７０３）。ＶＰＮ毎にルーティングテーブルが設定される（７０４）。

【００６８】ＶＰＮ識別子の設定は、インターフェースカードをパケット処理カードに装着する際に、インターフェースカードとパケット処理カード間で通信を行い、インターフェースカードが終端するＩＰパケットの下位レイヤのプロトコルを自動的に判定してパケット処理カードに通知するようにしてもよい。その通知された下位レイヤのプロトコルに対応して規定された識別情報を、ＶＰＮ識別子設定テーブルに自動設定することができる。

【００６９】以上、図１～図１４を用いて本発明のＶＰＮエッジルータの動作を説明した。これらに共通する動作フローを図１５に示す。

【００７０】ＶＰＮエッジルータは、ＬＡＮからＩＰパケットをカプセル化したパケットを受信すると（８０１）、ＶＰＮ識別子設定テーブルを検索し（８０２）、受信パケットのＶＰＮ識別子を決定する（８０３）。Ｖ

ＰＮ識別子としては、ＶＰＩ、ＶＣＩ等、論理的なチャネル識別子を用いるが、収容する下位プロトコルに応じて、これと物理インタフェース番号等とを組み合わせて使用してもよい。次に、決定したＶＰＮ識別子を検索キーとして、ＶＰＮ識別テーブルを検索し（８０４）、受信パケットが属するＶＰＮを決定する（８０５）。例えば、ＶＰＮ識別子がＶＰＩ、ＶＣＩである場合には、受信パケットに割り当てられたＶＰＩ、ＶＣＩを検索キーとして、ＶＰＮ識別テーブルを検索し、受信パケットが属するＶＰＮを決定する。決定されたＶＰＮ用のルーティングテーブルを検索し（８０６）、出力方路および出力用カプセルヘッダを決定する（８０７）。

【００７１】

【発明の効果】本発明のルータを用いることにより、物理インターフェースに多重化されている論理的なチャネル番号を用いてＶＰＮを識別することができる。従って、物理回線を増やすことなく、収容するＶＰＮの数を増やすことができる。

【００７２】また、ルータが収容する複数のＬＡＮがそれぞれ異なるＩＰの下位プロトコルを用いる場合でも、それぞれのプロトコルに対応した適切なＶＰＮ識別子を設定することができるので、ＶＰＮ識別を行うことができる。

【図面の簡単な説明】

【図１】本発明のＶＰＮエッジルータを用いて構成したＶＰＮの一実施例を説明するための図である。

【図２】図１に示される実施例の変形例を説明するための図である。

【図３】図１に示される実施例の他の変形例を説明するための図である。

【図４】本発明のＶＰＮエッジルータの一構成例を示す図である。

【図５】パケットレイヤ処理部の一構成例を示す図である。

【図６】ＶＰＮ識別子設定テーブル（１５０）の一構成例を示す図である。

【図７】ＶＰＮ識別テーブルの一構成例を示す図である。

【図８】ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図９】本発明のＶＰＮエッジルータ装置の他の構成例を示す図である。

【図１０】パケット処理カードにＡＴＭ用インターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１１】パケット処理カードにＰＯＳ用インターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１２】パケット処理カードに時分割多重回線用のインターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１３】パケット処理カードに異なる下位プロトコル用のインターフェースカードが収容される場合における、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの一構成例を示す図である。

【図１４】パケット処理カードの設定手順の一例を示す図である。

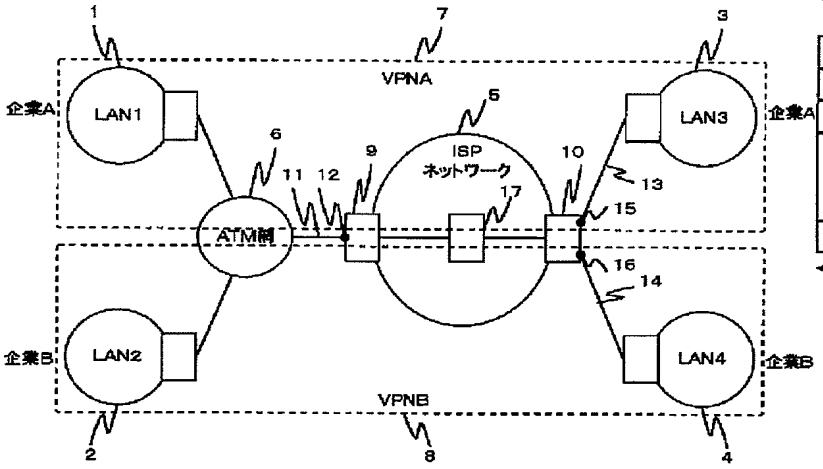
【図１５】本発明のＶＰＮエッジルータの動作フローを示すフローチャートである。

【符号の説明】

５…ＩＳＰネットワーク、９…ＶＰＮエッジルータ、５０…制御部、５１…スイッチ、５２…パケットレイヤ処理部、５３、５４…下位レイヤ処理部、１０１、１０５…パケット転送処理部、１０２…ＶＰＮ識別・ルーティングテーブル検索処理部、１５０…ＶＰＮ識別子設定テーブル、１５１…ＶＰＮ識別テーブル、１５２…ルーティングテーブル、４００…ＡＴＭ用インターフェースカード、４０１…ＰＯＳ用インターフェースカード、４０７…パケット処理カード。

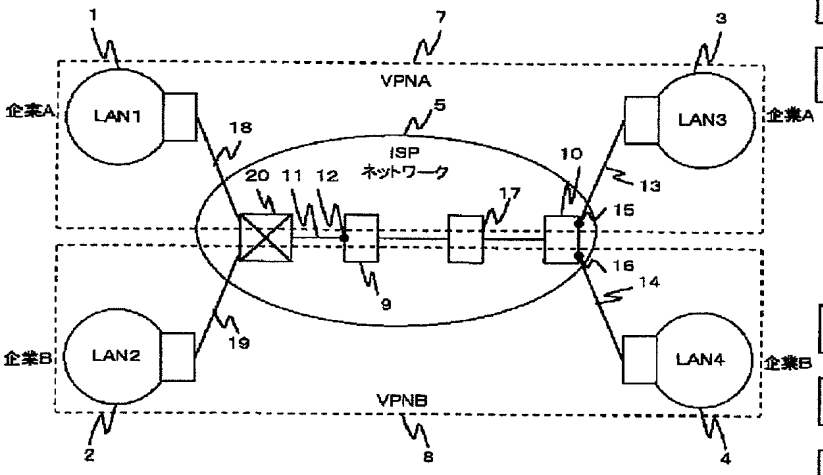
【図１】

図1




【図２】

図2




【図８】

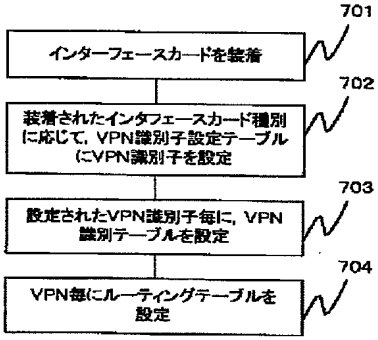
図8

| 300 宛先IPアドレス | 301 出力方路番号 | 302 出力カプセルヘッダ情報 |
|---|---|---|
| a. a. a. a | 10 | a |
| b. b. b. b | 11 | b |
| ⋮ | ⋮ | ⋮ |
| n. n. n. n | 15 | n |

検索キー　　検索結果

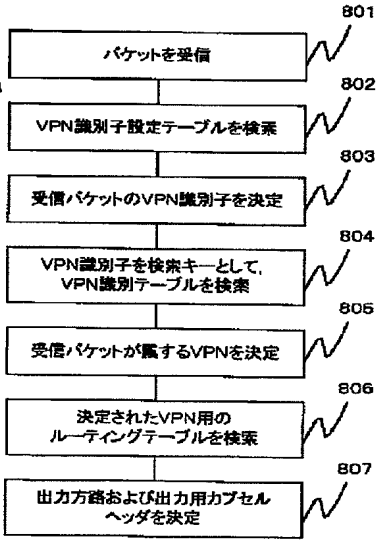
【図１４】

図14



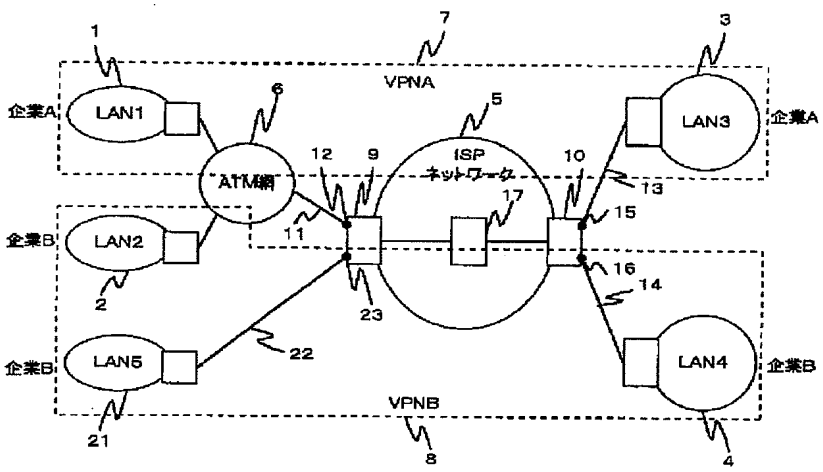

【図１５】

図15



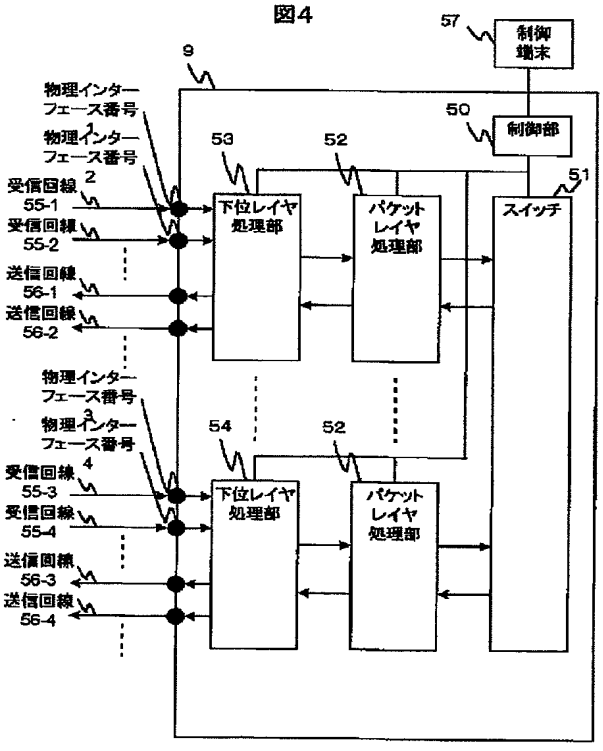
【図３】

図3



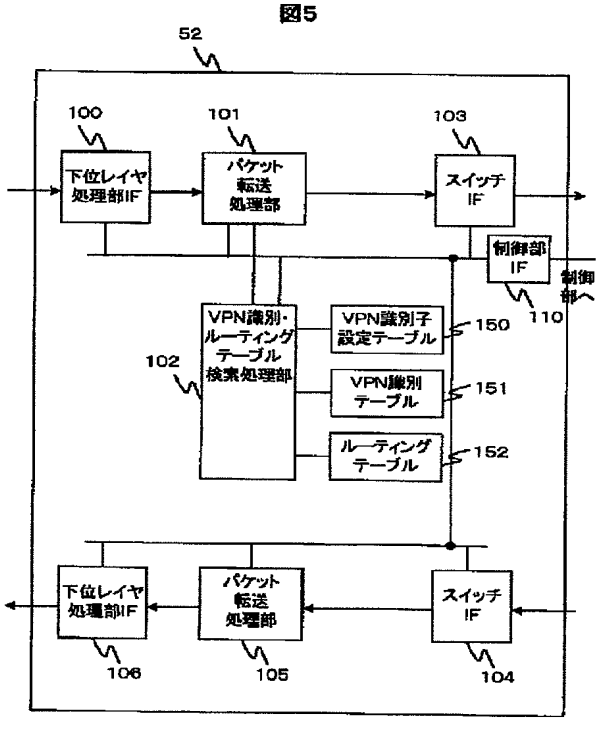

【図４】

図4



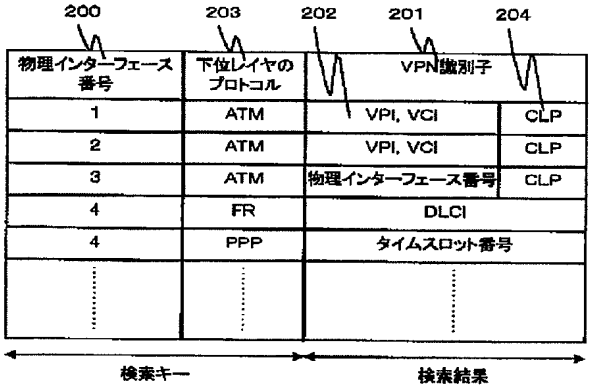

【図５】

図5



【図６】

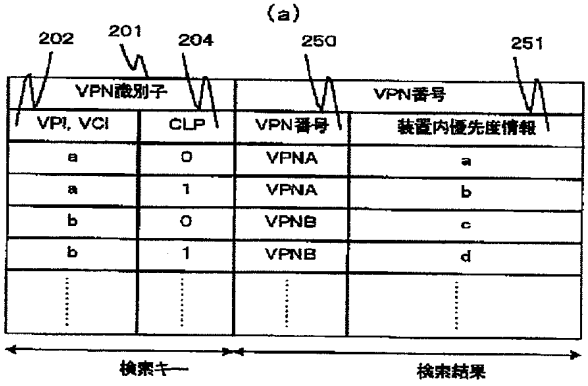
図6



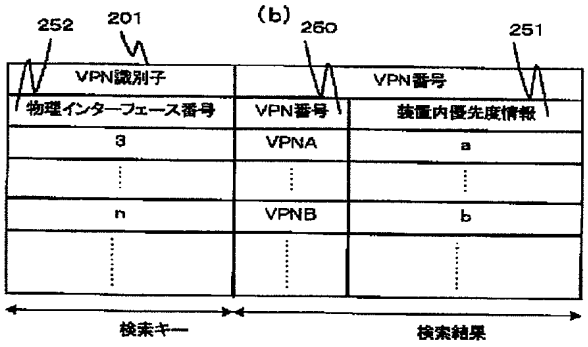

【図７】

図7

(a)

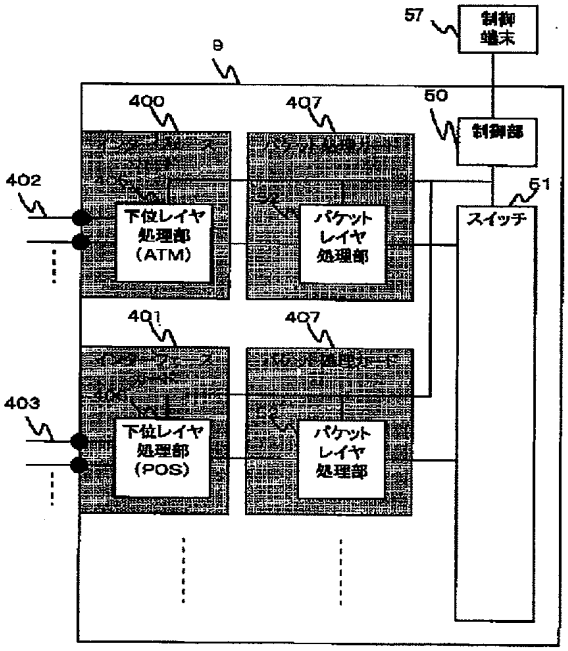



(b)



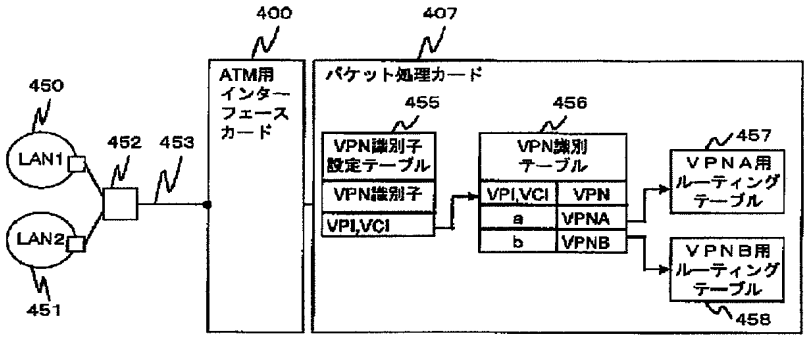

【図９】

図9



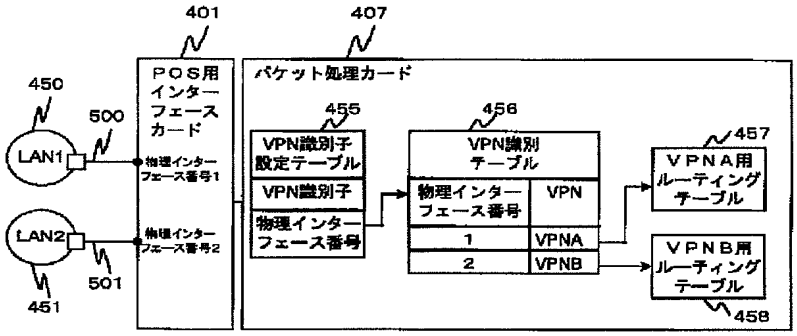
【図１０】

図10



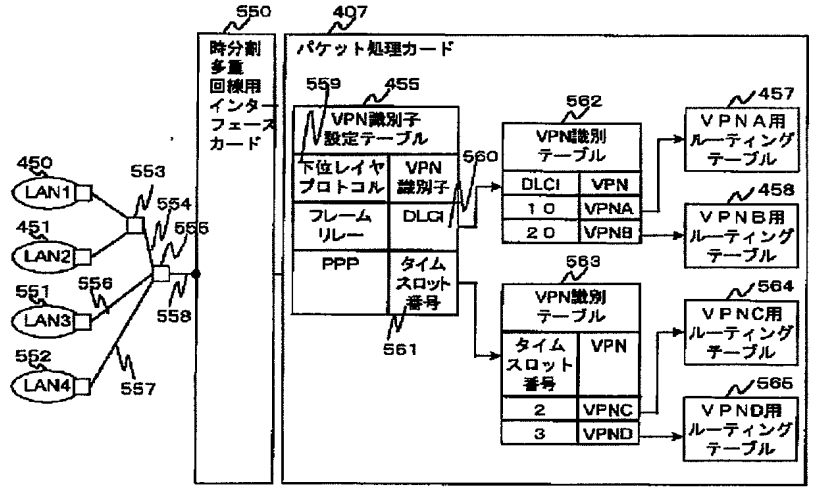

【図１１】

図11



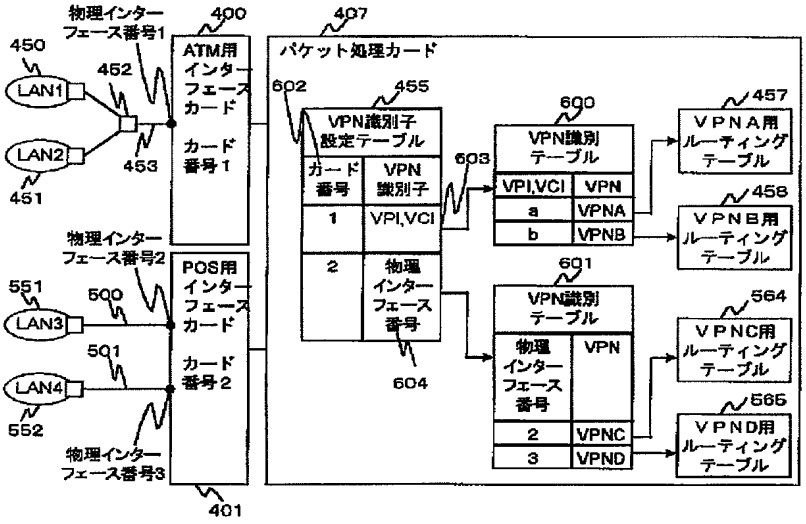

【図１２】

図12



【図１３】

図13




フロントページの続き

(72)発明者　須貝　和雄
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内

Ｆターム(参考)　5K030 GA04 HA08 HA09 HA10 HB14
HC01 HC14 HD03 KA05 LB05
LD17
5K033 AA04 CB08 DA06 DB12